AirTight WIPS

The Only True Wireless Intrusion Prevention System

Undisputed Global Leader in Wireless Security

- AirTight invented wireless intrusion prevention; owns 29 granted patents

Gartner on AirTight

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirTight Networks					x
Aruba Networks				x	
Cisco				x	
Fluke Networks				x	
Meraki			x		
Motorola				x	

AirTight WIPS is the only WIPS:

- Ever to receive the highest “Strong Positive” rating from Gartner – now two years in a row!
- Rated at the top by Gartner in all its six MarketScope reports on WLAN IPS

US DoD Approved

Common Criteria

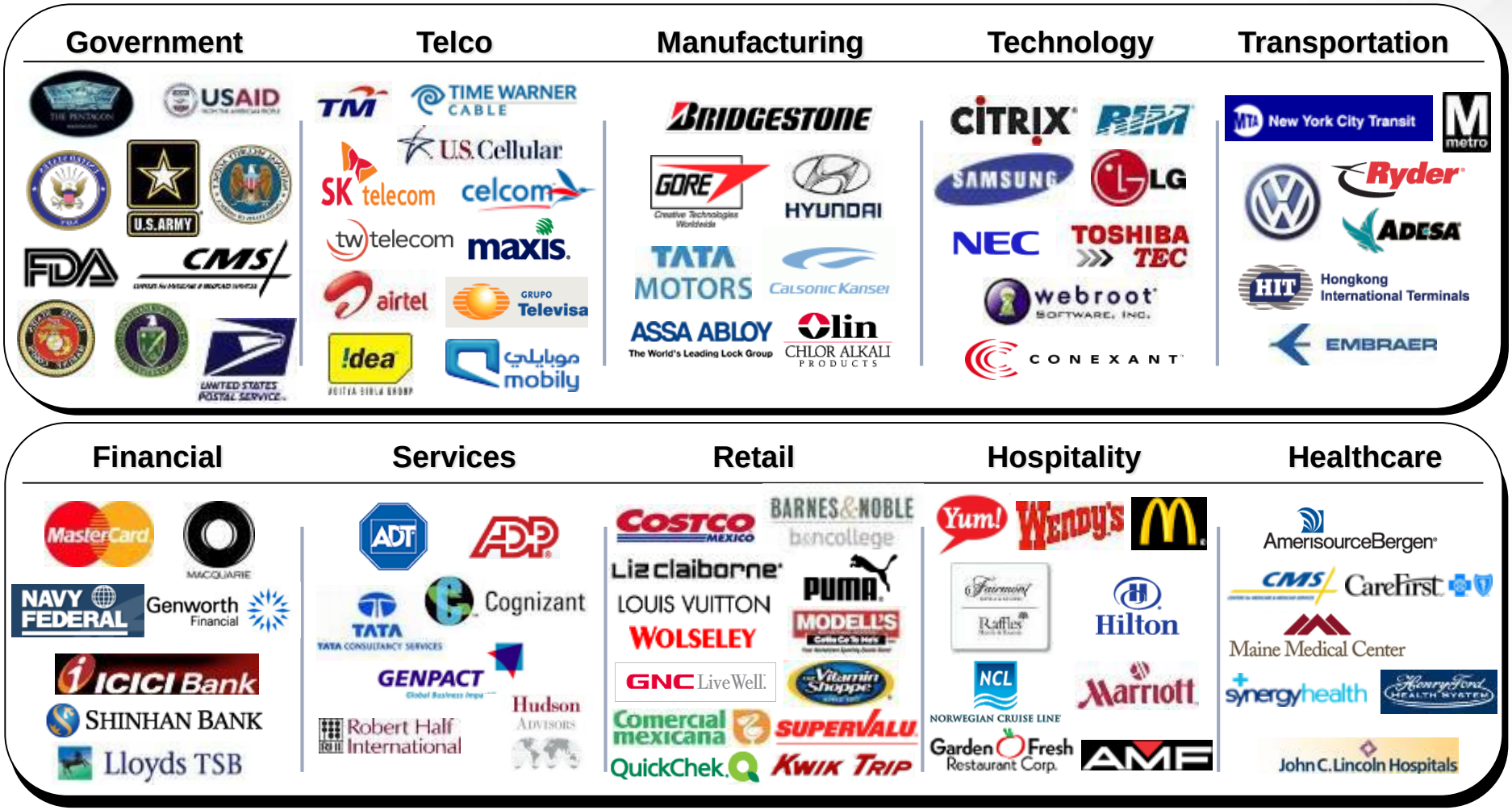
FIPS VALIDATED 140-2

DISA UC APL

AirTight WIPS is the only WIPS:

- Certified for Common Criteria EAL2+, FIPS 140-2 and DISA UC APL

Trusted by Thousands of Customers Worldwide



Wireless Security

(Re)Considering Wireless Security

What does not work?

A “No Wi-Fi” policy without enforcement

We don’t have “that” problem because…

TJX Breach – The Tip of the Iceberg

THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

TJX Hacker Charged With Heartland, Hannaford Breaches

By Kim Zetter August 17, 2009 | 2:34 pm | Categories: Breaches

The constellation of hacks connected to the TJX hacker is growing.

Albert "Segvec" Gonzalez has been indicted by a federal grand jury in New Jersey — along with two unnamed Russian conspirators — on charges of hacking into Heartland Payment Systems, the New Jersey-based card processing company, as well as Hannaford Brothers, 7-Eleven and two unnamed national retailers, according to the indictment unsealed Monday. Gonzalez, a former Secret Service informant, is already awaiting trial over his involvement in the TJX hack.

According to the court document, the hackers allegedly stole more than 130 million credit and debit card numbers (.pdf) from Heartland and Hannaford combined. Prosecutors say they believe these breaches constitute the largest data-breach and identity-theft case ever prosecuted in the United States. They're investigating other breaches and have not ruled out Gonzalez's involvement in even more intrusions.

Additional breaches

Marshalls. SPORTS AUTHORITY

Heartland PAYMENT SYSTEMS 7-ELEVEN

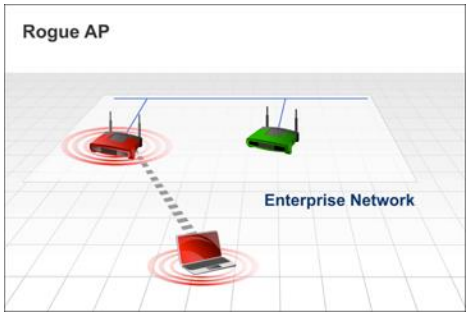
OfficeMax

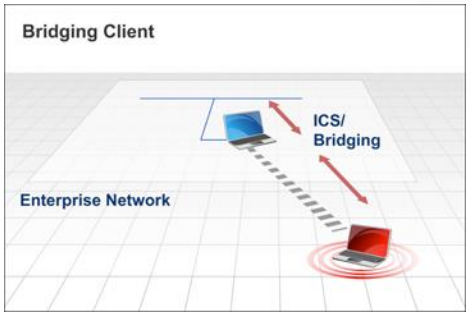
BARNES & NOBLE BOOKSELLERS BJ's WHOLESALE CLUB

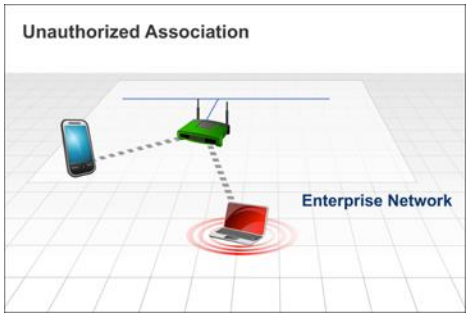
FOREVER 21 DSW

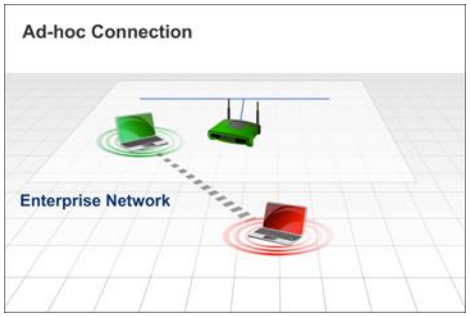
BOSTON MARKET Home Style Meals Hannaford

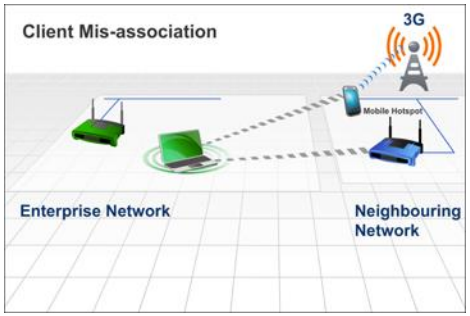
Top Ten Wireless Threats

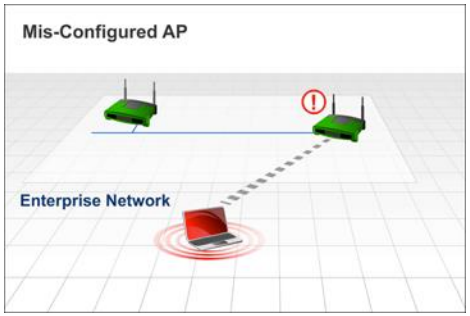


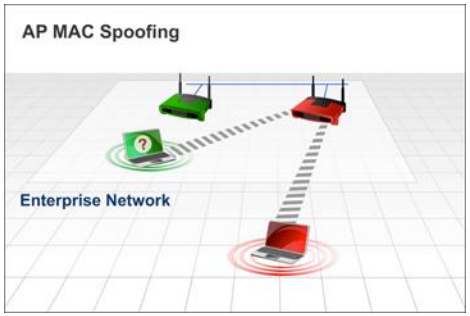


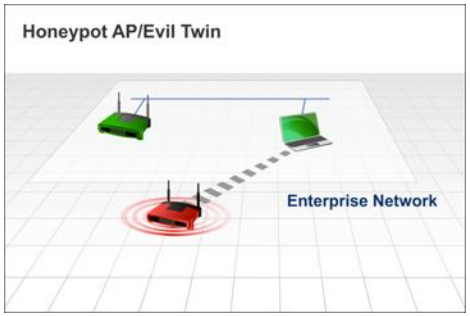


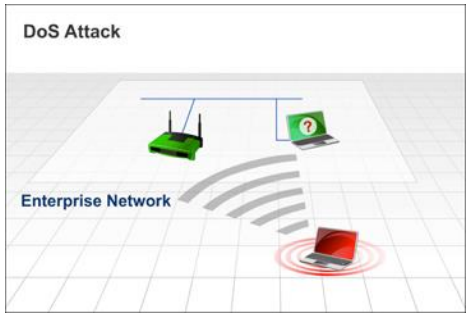












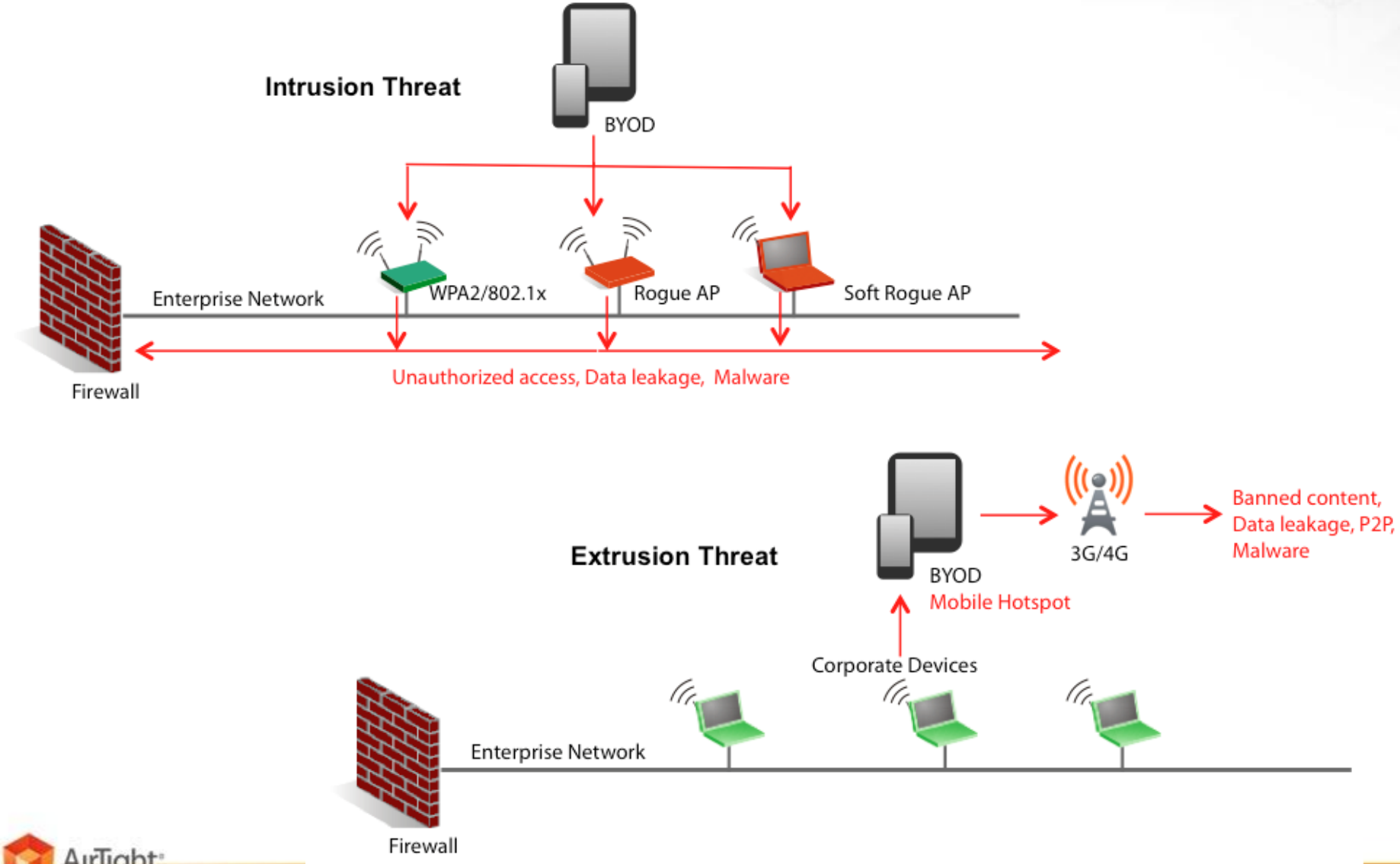
AirTight® NETWORKS

Is your network security at risk from BYOD?

Managing the “Unmanaged”

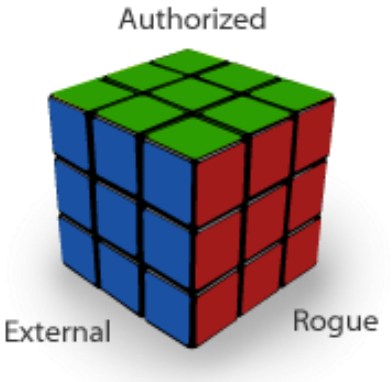
WPA2/802.1x cannot prevent unauthorized devices from accessing the enterprise network

Managing the “Unmanaged”



Why AirTight WIPS?

AirTight WIPS – The Only True WIPS



Automatic
Device Classification

Comprehensive
Threat Coverage

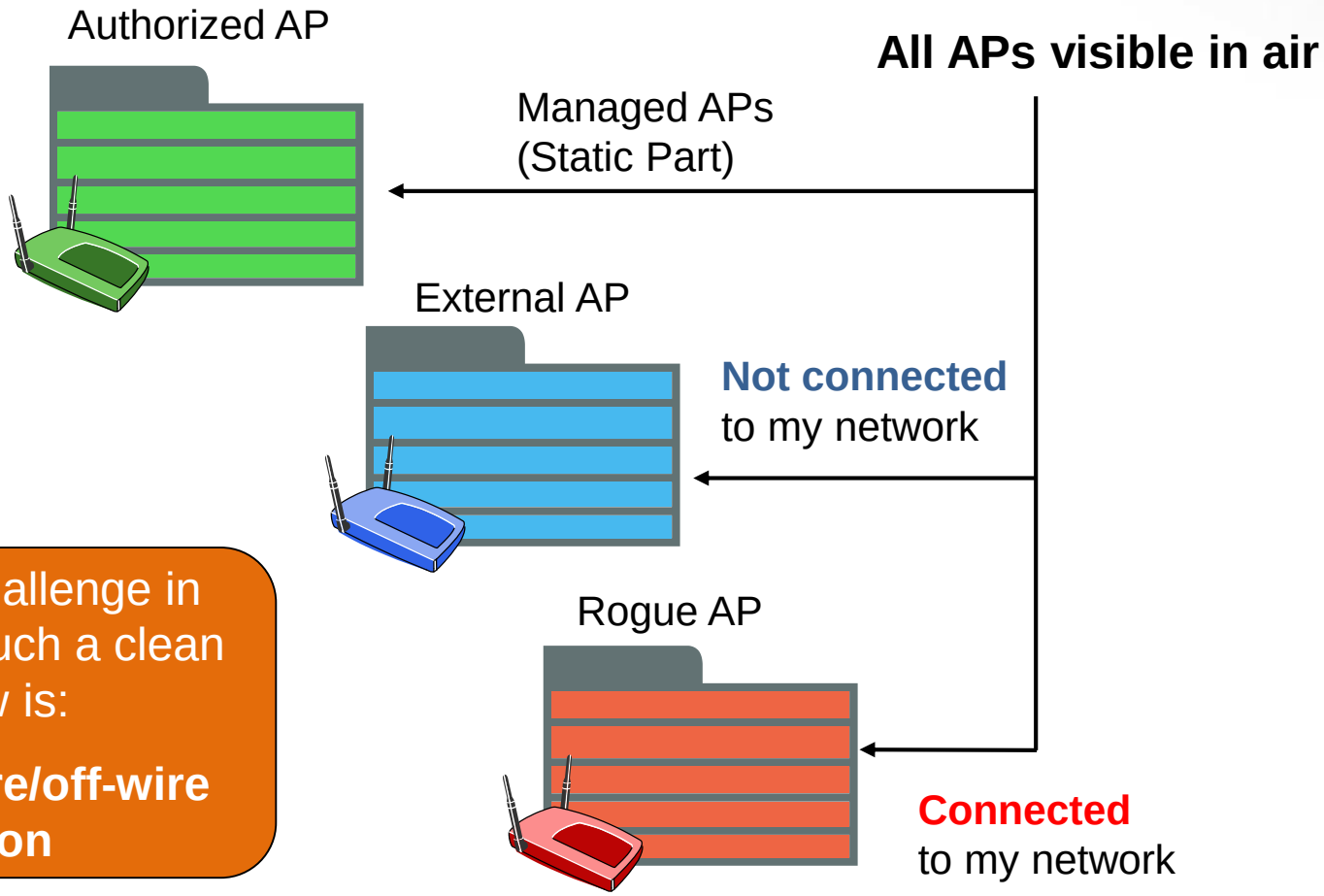
Reliable
Threat Prevention

Accurate
Location Tracking

BYOD
Policy Enforcement

Automated
Compliance Reporting

AirTight's Accurate Automatic Device Classification



The biggest challenge in implementing such a clean workflow is:

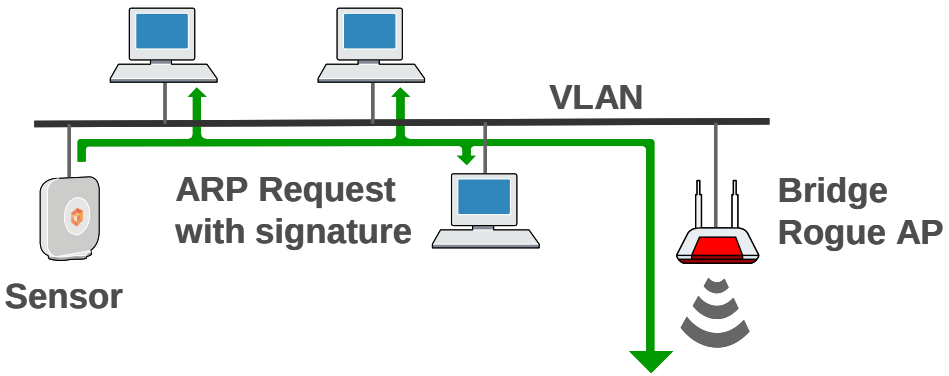
Robust on-wire/off-wire detection

AirTight's Patented Marker Packet™ Technique

Definitive "on-wire / off-wire" test

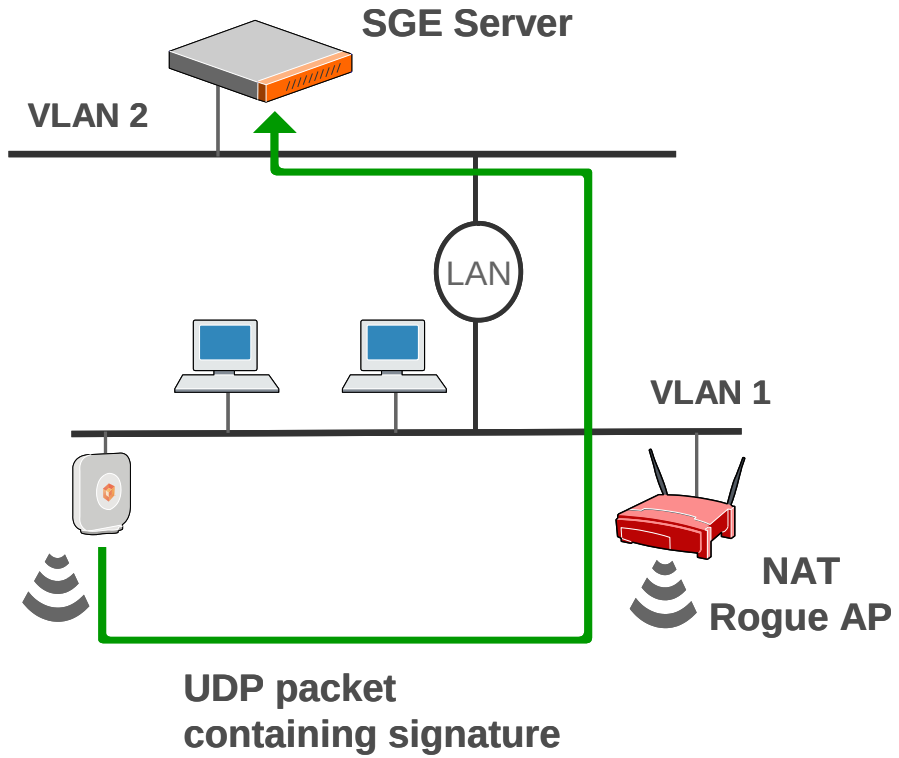
ARP Request Marker Packet

Sensor sends ARP requests with signatures on the wire and detects if any get forwarded onto the wireless side



UDP Reverse Marker Packet

Sensor sends UDP packets with signatures in the air and server detects if any get forwarded onto the wire

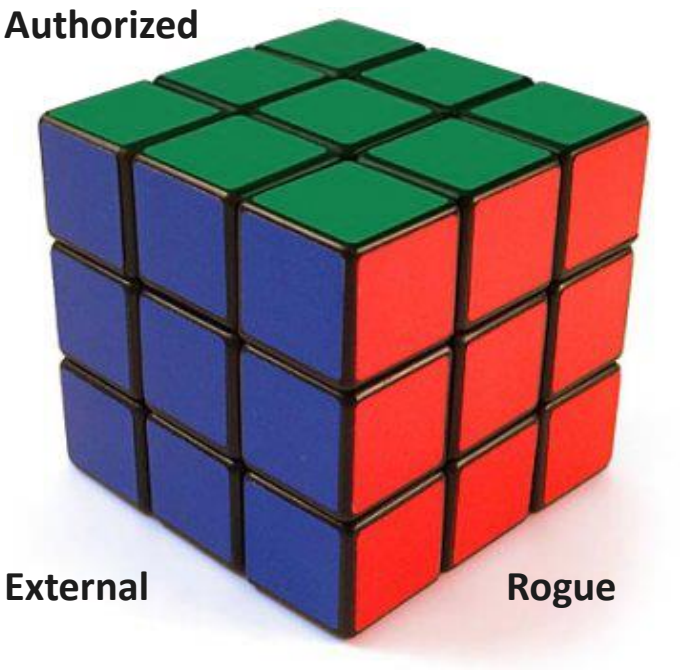


Head-to-Head Comparison Of Rogue AP Detection

Criteria	Marker Packets	MAC Correlation
1. False negative on NAT APs	Never	Often
2. False positive on neighbor AP	Never	Often
3. Latency of detection	Low (few minutes)	High (tens of minutes)
4. Configuration, maintenance	Zero	High
5. Scalability	Infinite	Poor
6. Manual intervention for classification	None	Extensive

Automatic Device Classification

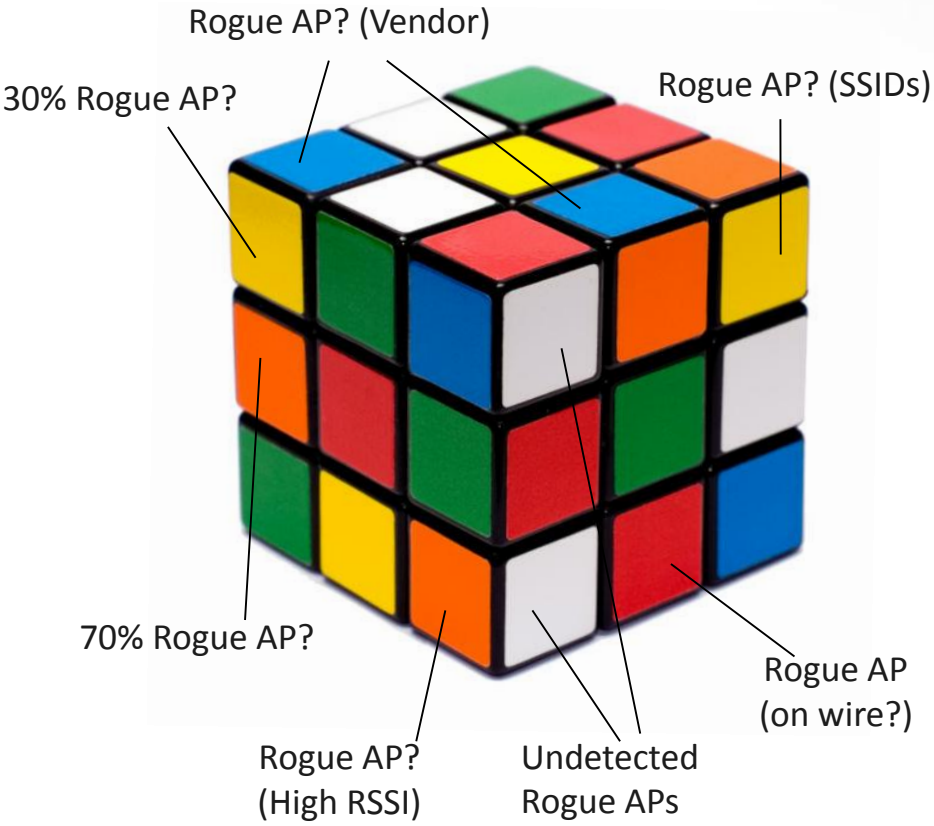
AirTight WIPS



Works "out of the box"

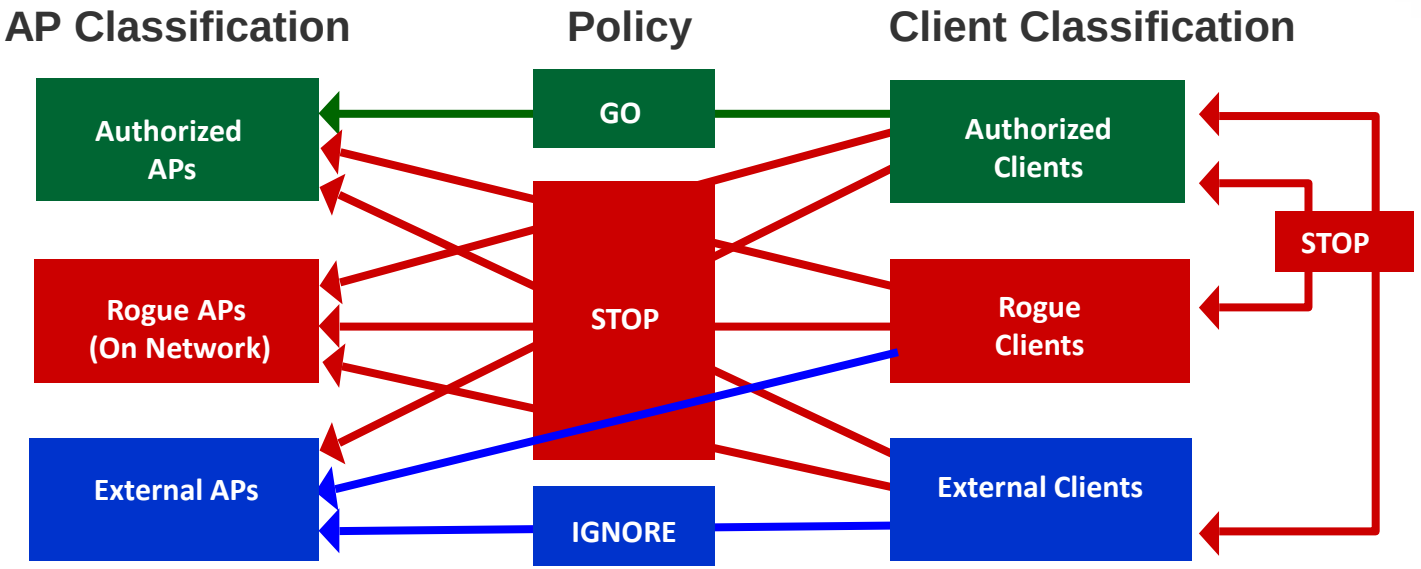
Rooted in active on-wire/off-wire detection

Other WIDS solutions



Require users to configure complex rules and marred with false alarms

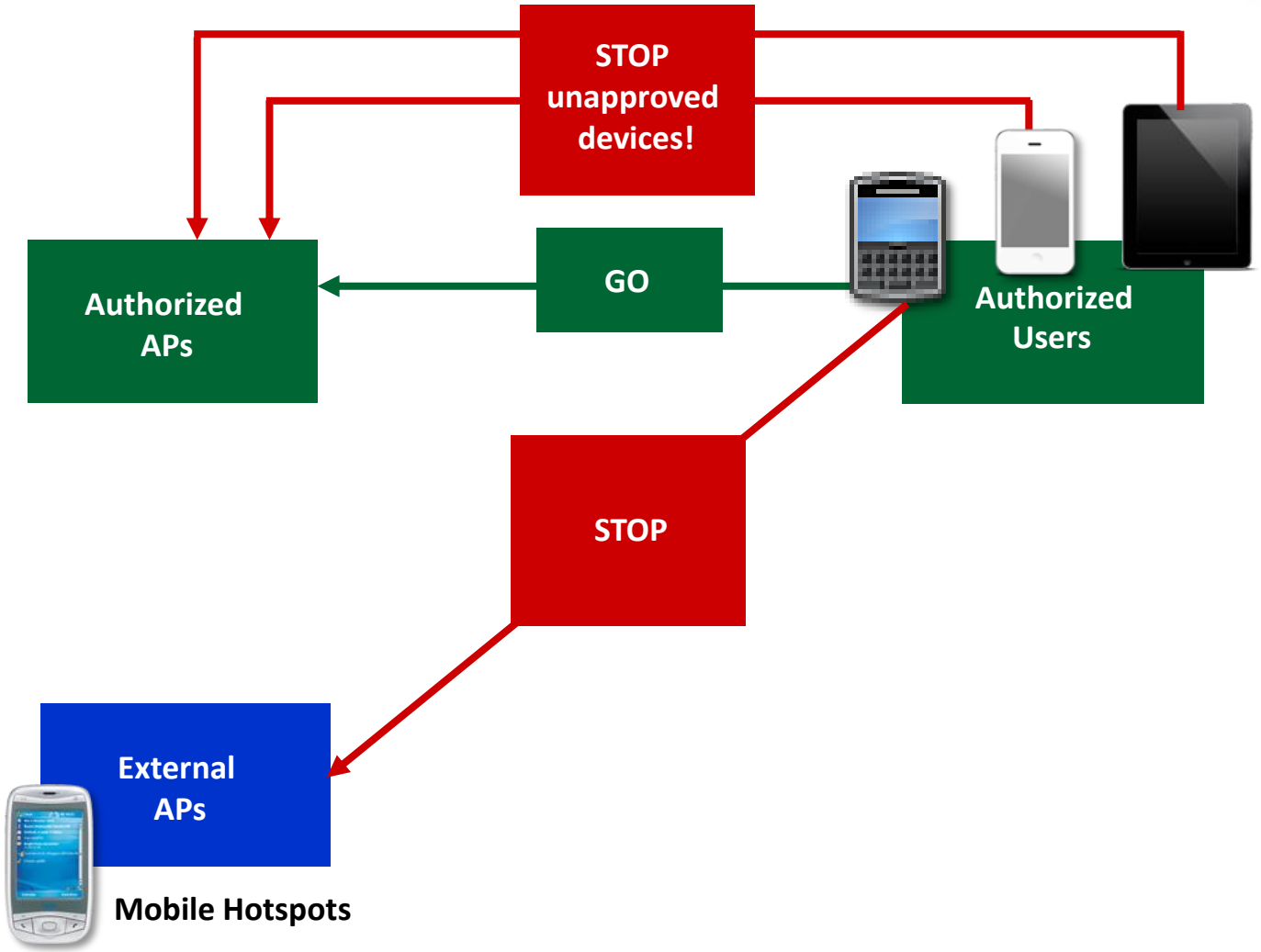
AirTight's 24/7 WIPS Protection



AUTOMATICALLY DETECTS AND BLOCKS RED PATHS!

With this in place, your network is protected from all types of wireless threats, vulnerabilities and attack tools!

Extending the WIPS for BYOD Policy Enforcement

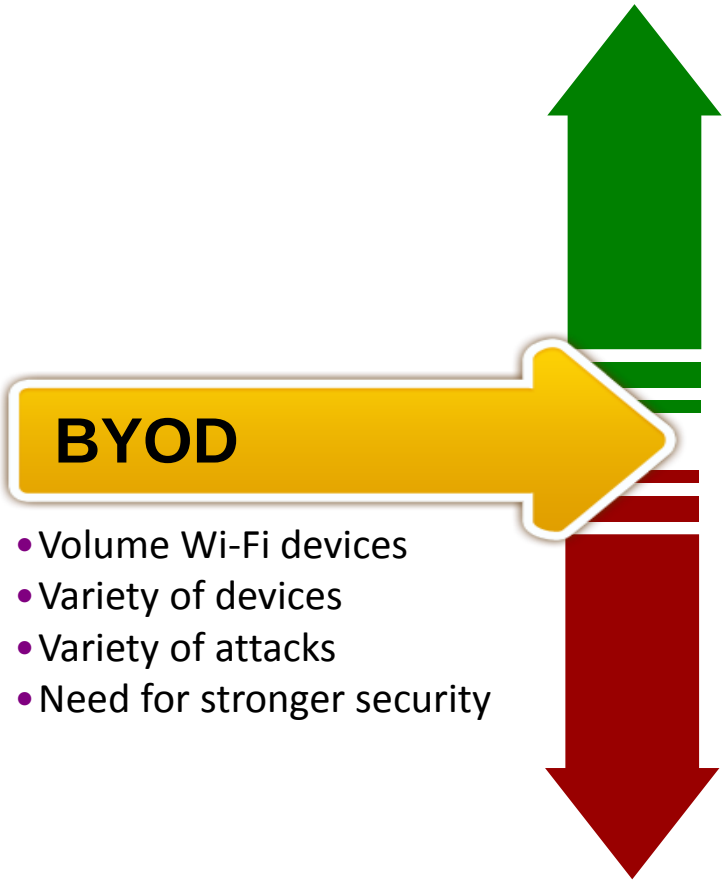


Automatic Device Fingerprinting and Classification

- MDM and NAC are unable to provide the first line of defense
- WIPS complements these solutions to fully automate secure BYOD

Android	30:39:26:4B:86:C1	30:39:26:4B:86:C1
Blackberry	BLACKBERRY-9FC8	30:69:4B:9C:FE:F7
Blackberry	BLACKBERRY-3300	40:6A:AB:E3:BA:C3
iPad	Var	74:E1:B6:BE:4B:AD
iPad	Sushmas-iPad.lo	FC:25:3F:AA:2E:AC
iPad	ATN	44:2A:60:9B:A1:C8
iPhone	Louiss-iPhone.l	58:1F:AA:61:A7:F7
iPhone	iPhone	00:1C:B3:65:73:94
iPhone	LAP119-PC	0C:77:1A:3B:42:0D
iPod-Touch	NP-	00:26:BB:BA:C7:A7
Windows-Mobile	Karan-HTC_90:11:1D	F8:DB:7F:90:11:1D
[illegible]	Nokia_2[illegible]	[illegible]C:E9:07:29:[illegible]

BYOD Amplifies AirTight WIPS Advantages



- Volume Wi-Fi devices
- Variety of devices
- Variety of attacks
- Need for stronger security

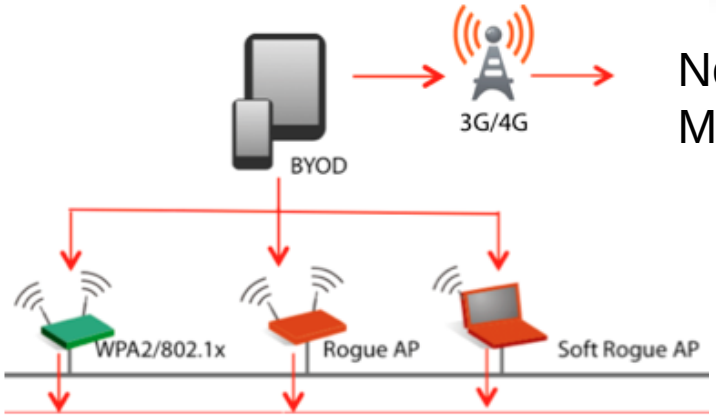
AirTight Strengths

- Automatic, accurate device classification
- Automatic, reliable prevention
- Zero false alarms
- Ease of use

Limitations of “checkmark WIDS”

- Unreliable signature approach
- Manual inspection not practical
- Unreliable prevention
- Lack of automation
- Complex, difficult to manage

MDM ≠ Network Security

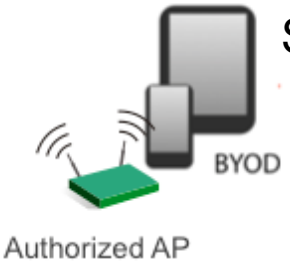


No visibility into Rogue APs, Soft Rogues, Mobile Wi-Fi Hotspots

Scope limited to “managed” devices that run MDM agent

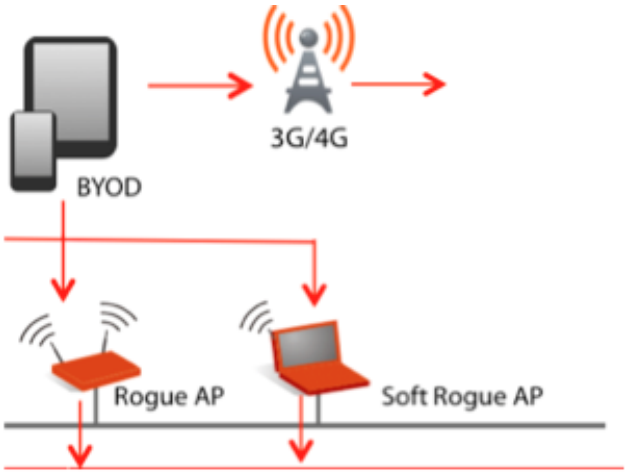
What is the incentive to install MDM agents on personal devices?

NAC ≠ Wireless Security



Scope limited to BYOD on “managed” WLAN

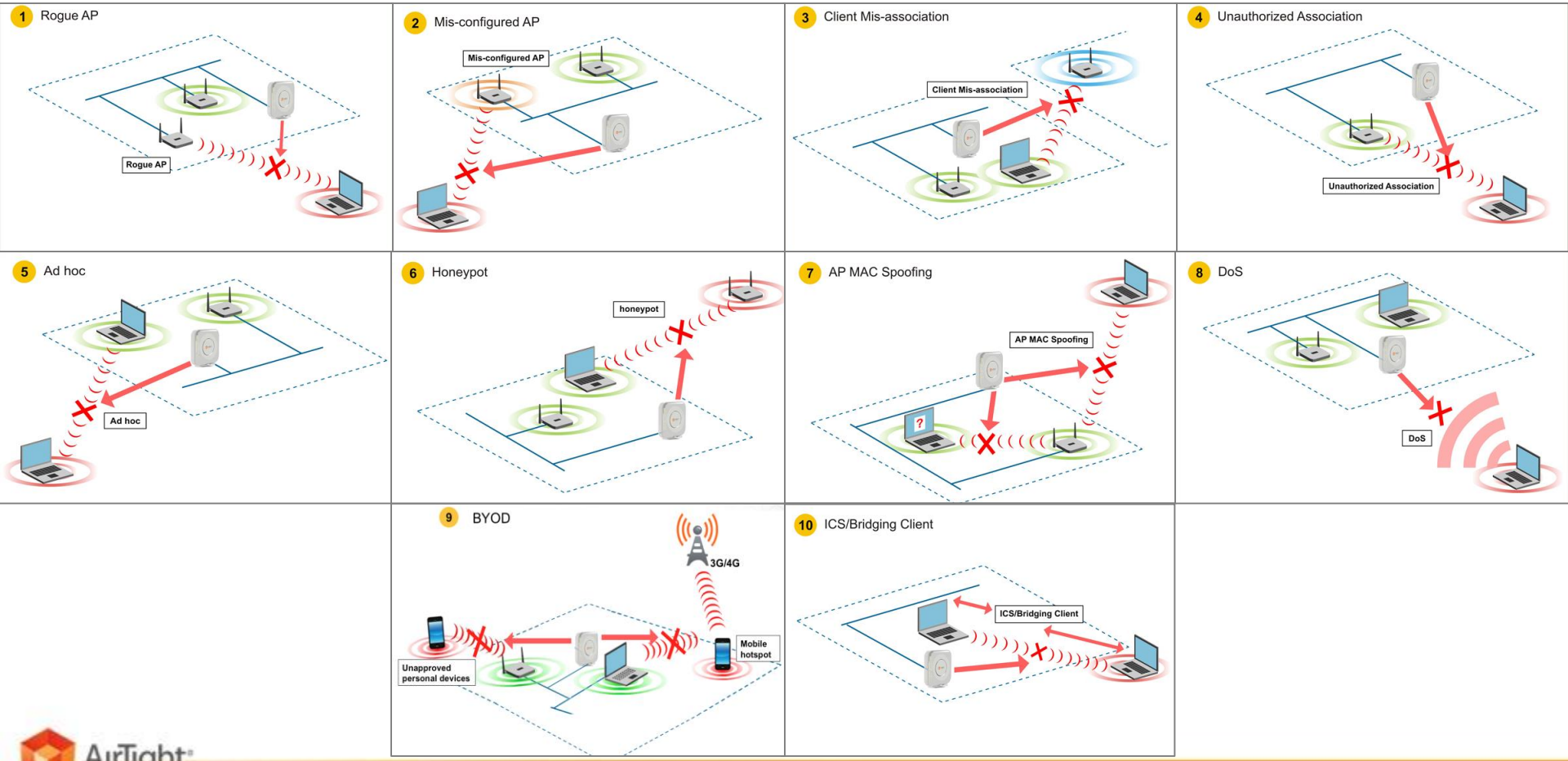
Cannot block Rogue APs, Soft Rogues, Mobile Wi-Fi Hotspots



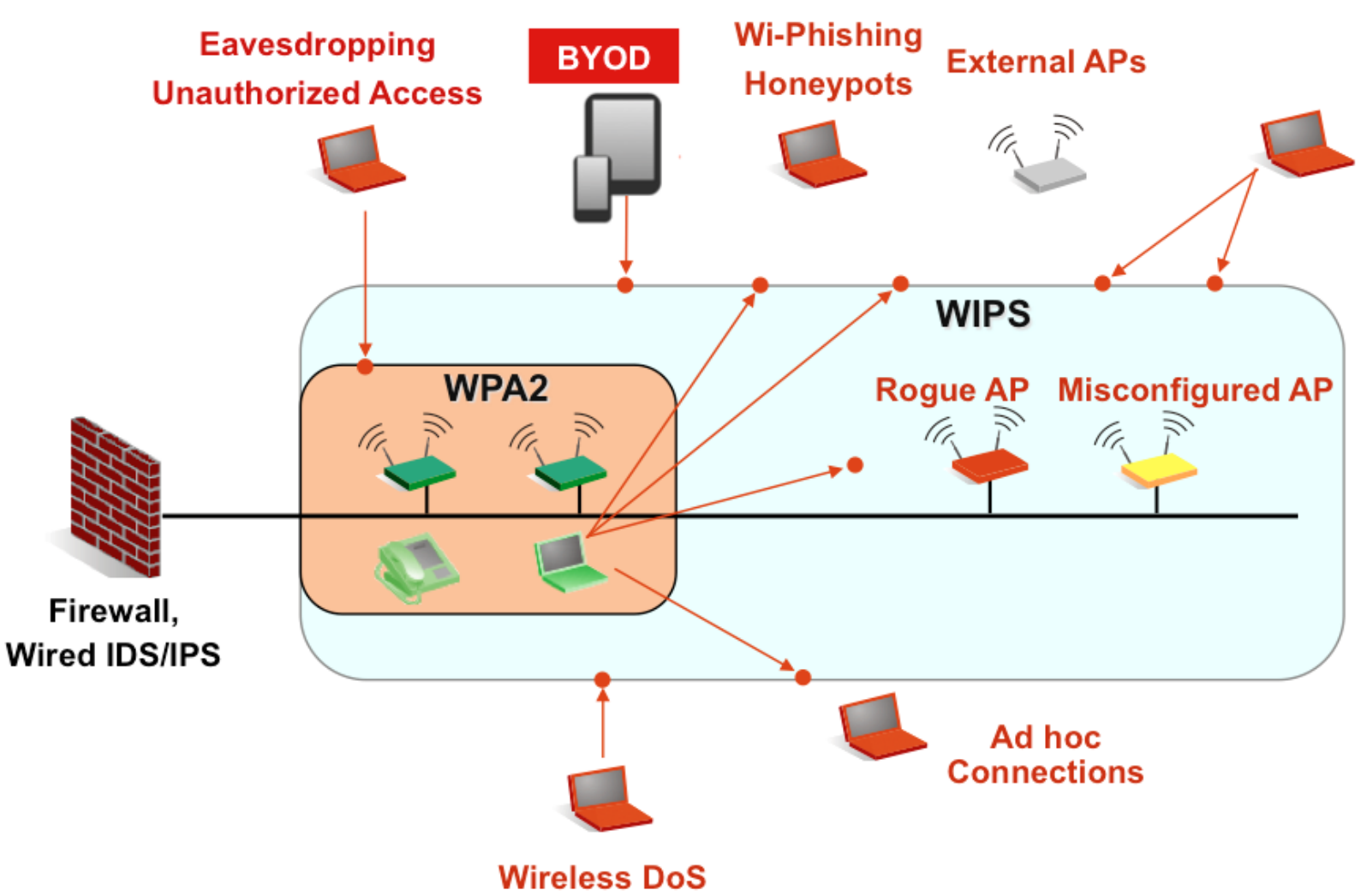
Suffers from “blind spots” – unauthorized Wi-Fi devices connecting via authorized devices

Comprehensive Protection with AirTight WIPS

- Surgical threat prevention without interfering with legitimate communication (yours or your neighbor's)
- Simultaneous prevention of multiple threats across multiple channels

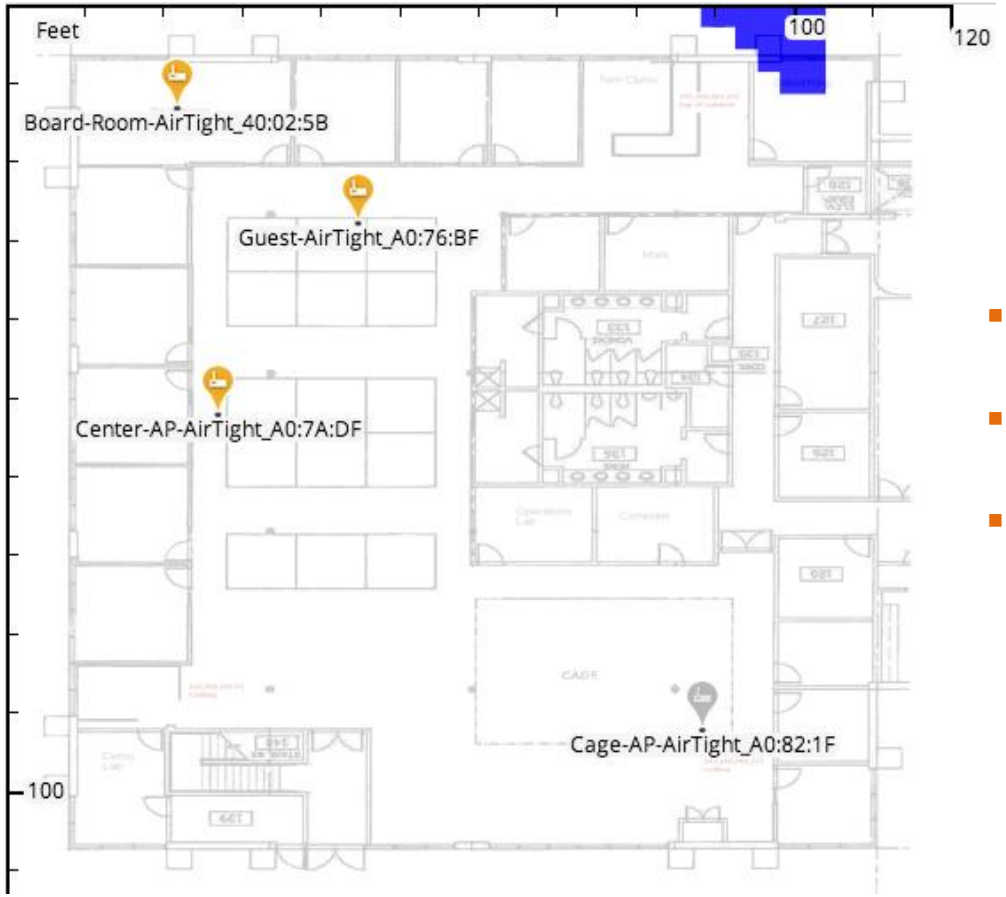


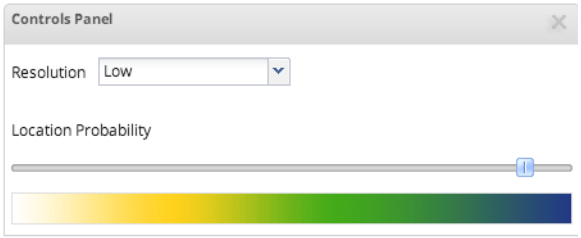
Comprehensive Protection with AirTight WIPS



AirTight's Accurate Location Tracking

Real Time and Historic

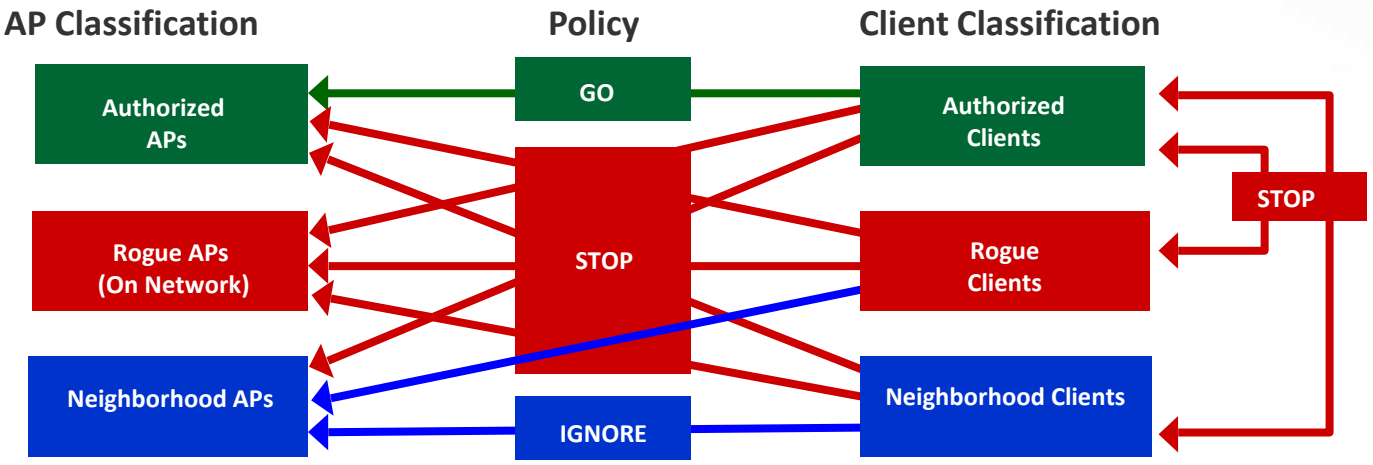




- No need for RF site survey
- No search squads to locate Wi-Fi devices
- Definitive location tracking within 10-15 ft.

Compare that to Other WIDS Solutions

AirTight Takes a Fundamentally Different Approach



With this in place, your network is protected from all types of threats, vulnerabilities and attack tools!

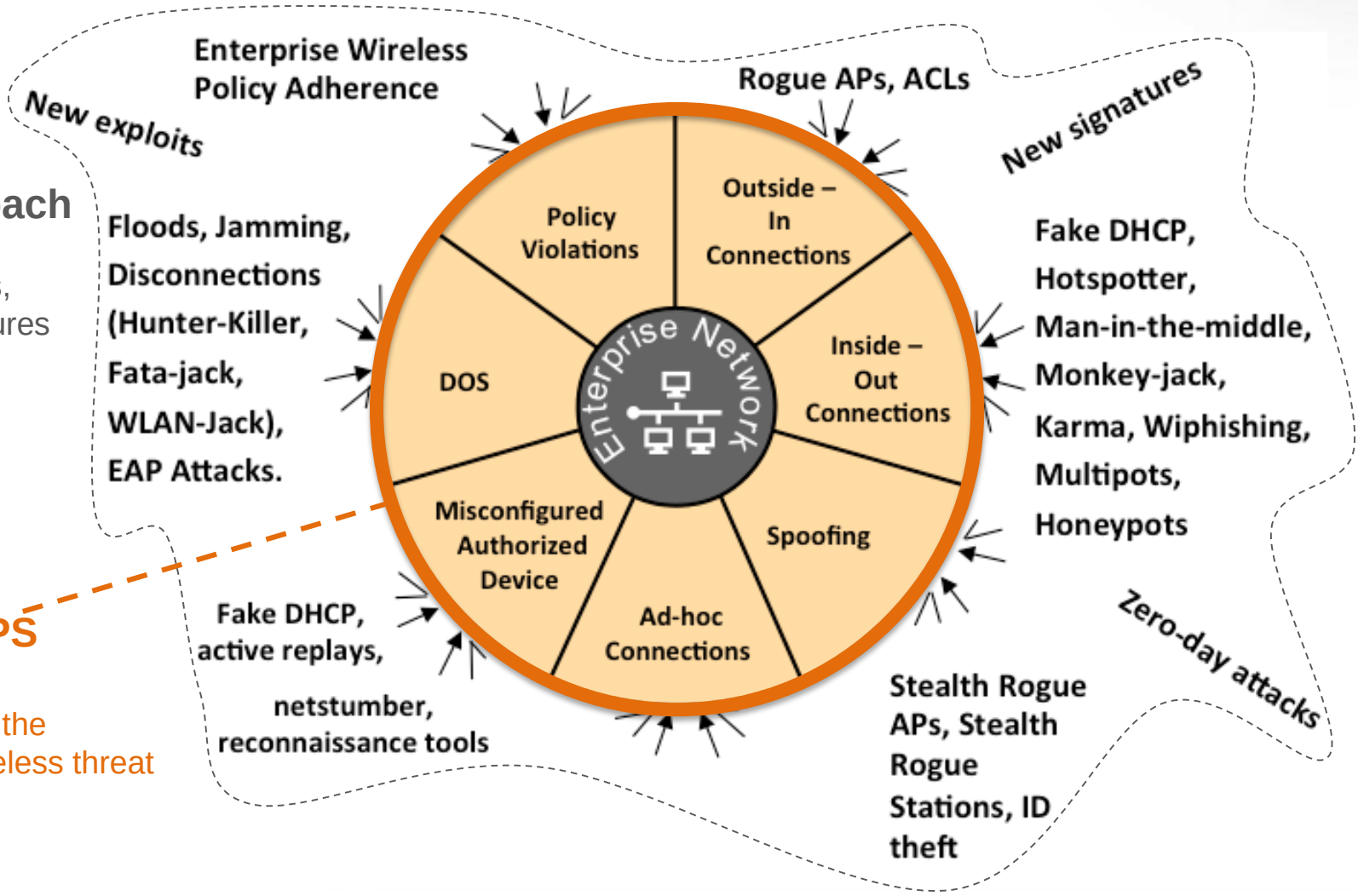
Competition

- Require user to configure and maintain classification rules
- Large number of events using signature matching and anomaly thresholds
- Prone to false alarms, require continuous manual intervention
- Unreliable for automated threat prevention
- Classic problems of signature approach: Incomplete and changing signatures
- Minimal “zero-day attack” protection

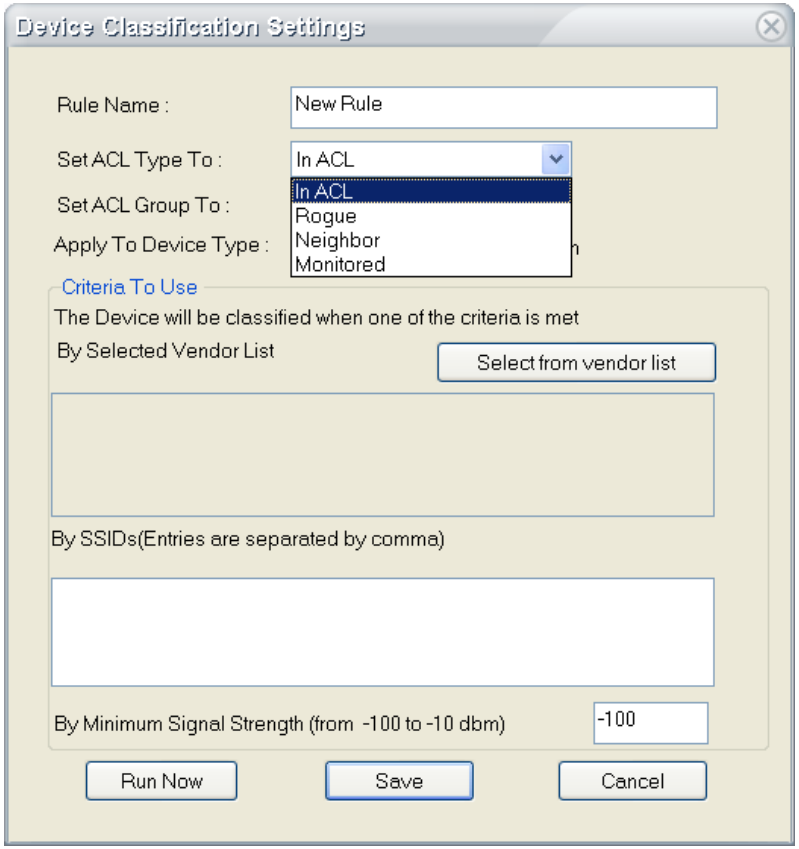
AirTight Takes a Fundamentally Different Approach

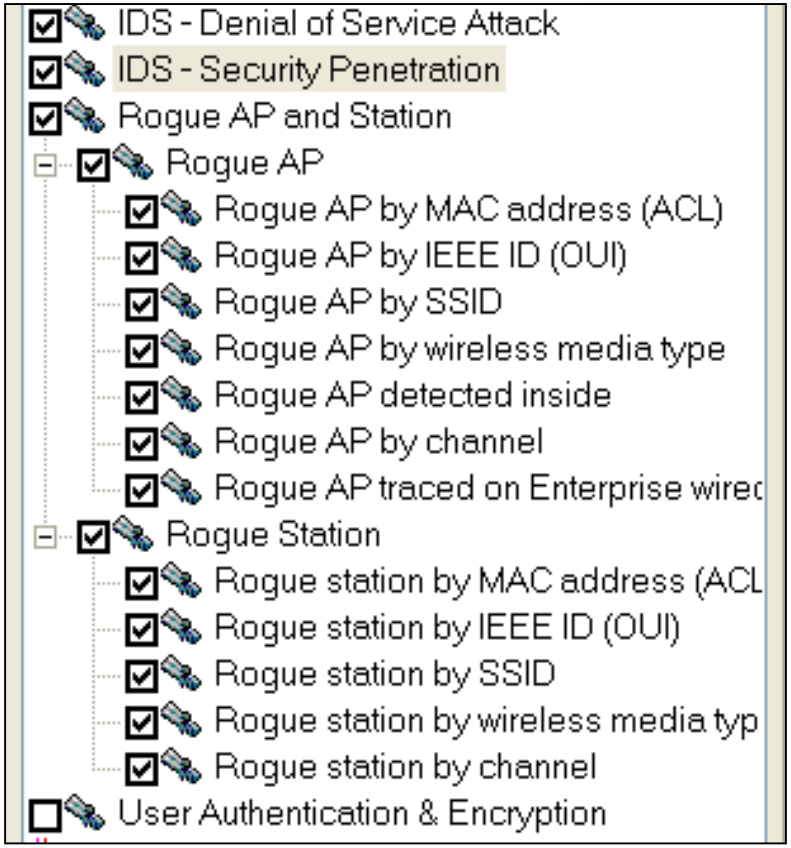
Prevalent WIDS Approach
Cat and mouse chase of exploits, tools and signatures

AirTight WIPS Approach
Protects against the fundamental wireless threat building blocks

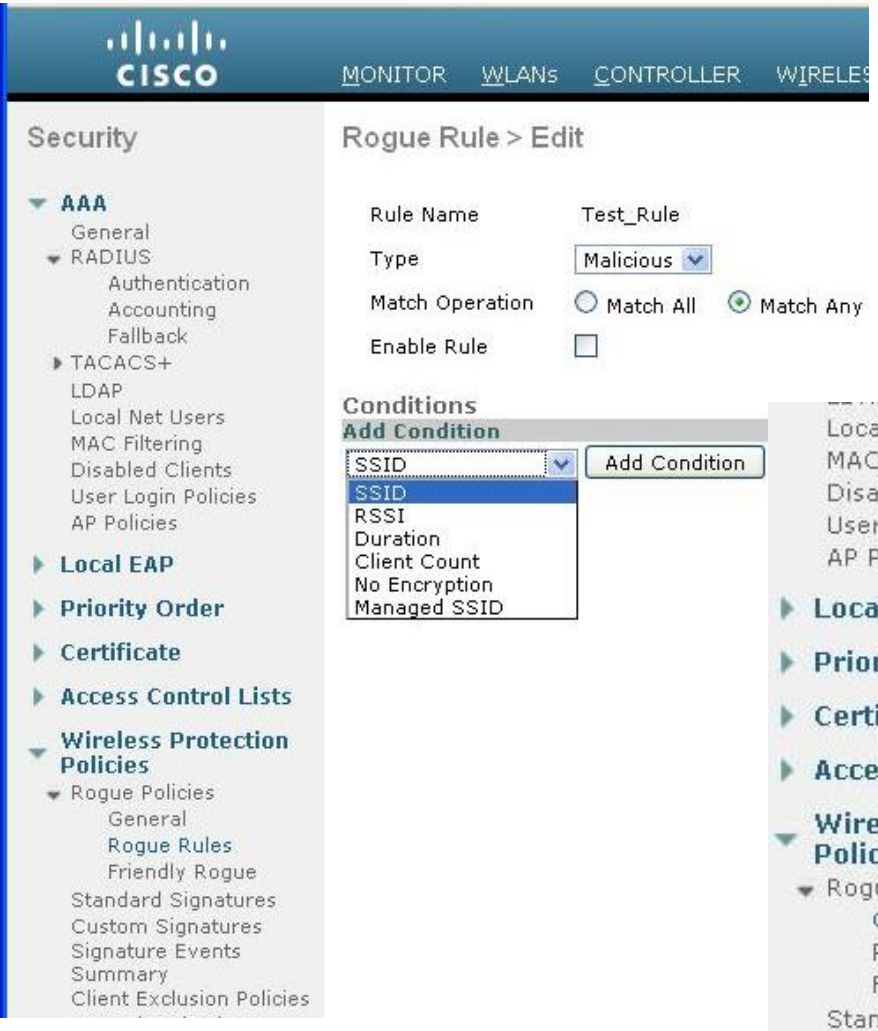


AirMagnet (Fluke Networks)





Cisco Adaptive WIPS



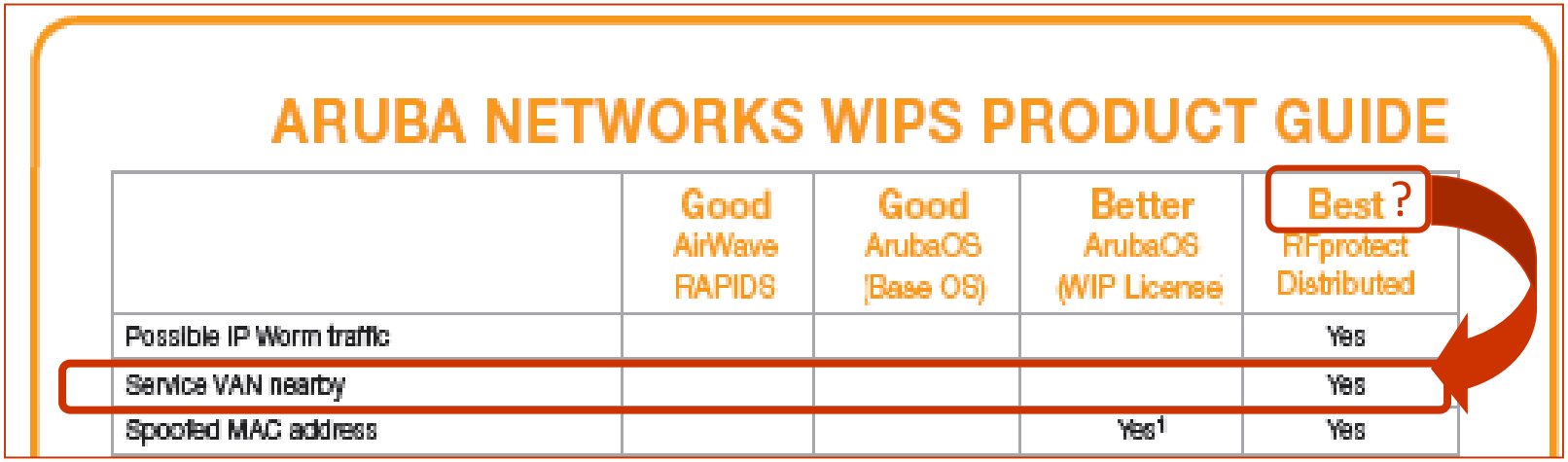
Many WLAN vendors offering “so-called WIPS” recommend their customers to NOT turn on automatic threat prevention!

Cisco Adaptive WIPS

Arbitrary Threshold and Packet Count Based Signatures to Hide False Alarms

DoS Detection Type	Alarm Threshold (PPM)	Alarm Interval (Sec)	Enabled
Probe Request	12000	60	☑
Probe Response	24000	60	☑
(Re)Association Request	6000	60	☑
Association Response	2400	60	☑
Disassociation	1200	60	☑
Authentication	6000	60	☑
De-authentication	1200	60	☑
EAP over LAN (EAPOL)	6000	60	☑

Aruba Networks – Petty Signatures to Hide False Alarms



ARUBA NETWORKS WIPS PRODUCT GUIDE

	Good AirWave RAPIDS	Good ArubaOS (Base OS)	Better ArubaOS (WIP License	Best ? RFprotect Distributed
Possible IP Worm traffic				Yes
Service VAN nearby				Yes
Spoofed MAC address			Yes[1]	Yes

Motorola AirDefense

Administrator has to define complex signature-based rules for wireless threat detection

MAC	***Signal Strength***	***Connectivity***
IP Address	***Protocol***	***Association***
Vendor	***Authorization***	***Key Generation***
Channel	***802.X Username***	***Specific EAP Type***
SSID	***Last Seen***	***Encryption***

Excerpt from the Motorol AirDefense User Guide

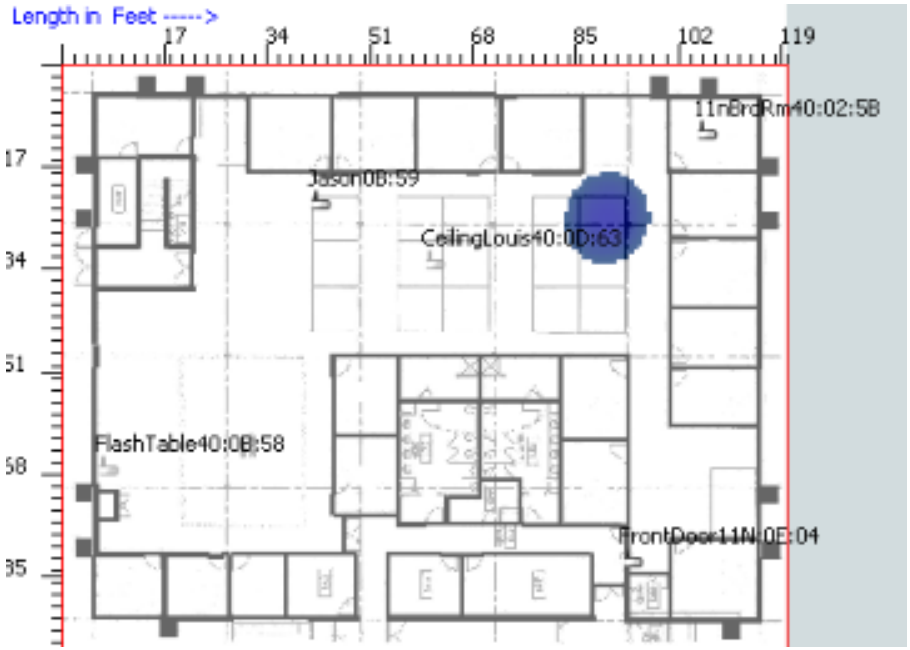
8.5.3.3 Scheduled

Because auto-classification places a minor burden on the system, AirDefense, Inc. recommends that you schedule auto-classification to occur only once or twice a day.

8.5.4.2 Action Rules

The Action Rules tab of the Auto Classification page lets you create a very specific set of rules for classifying devices. **The more criteria you include, the more accurate the resultant classification will be, and the less likely it is that a device will be mis-classified.**

Location Tracking



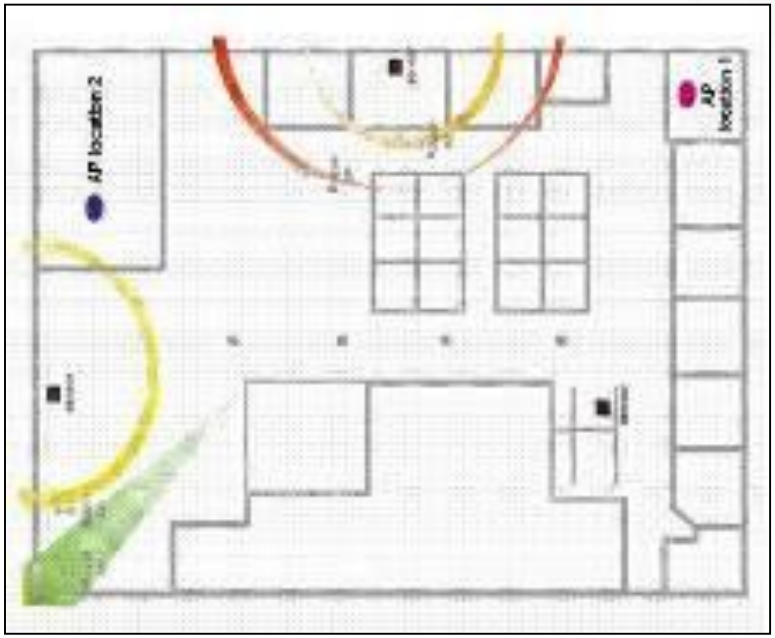
Stochastic RF Triangulation with Fingerprinting

Self adjusting to signal variations due to TX power fluctuations, antenna orientation and RF obstructions

Does not require site survey for calibration

Displayed as location probability distribution map

Competition



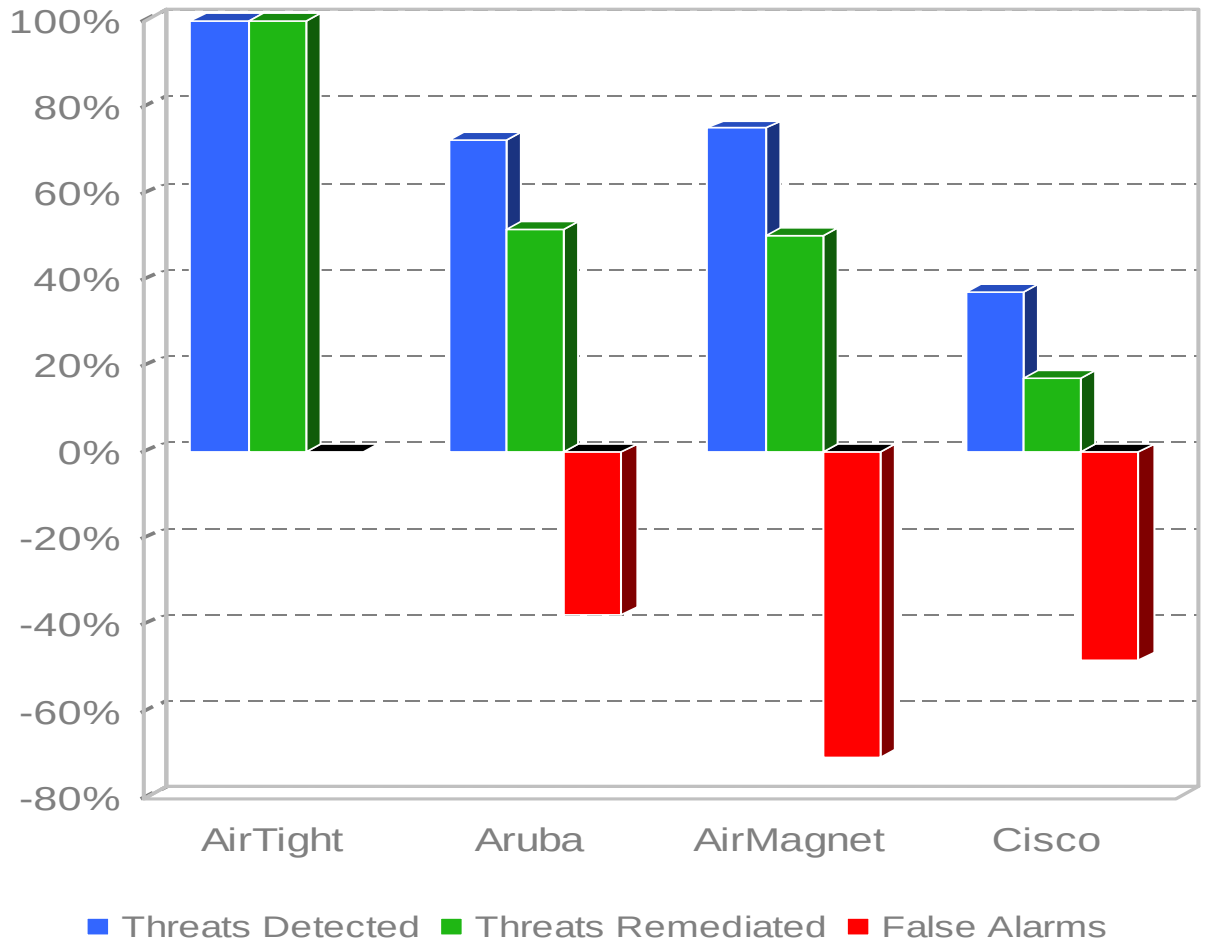
Simple RF Triangulation

Received signal strength used to estimate distance to the device and location estimated as intersection of circles

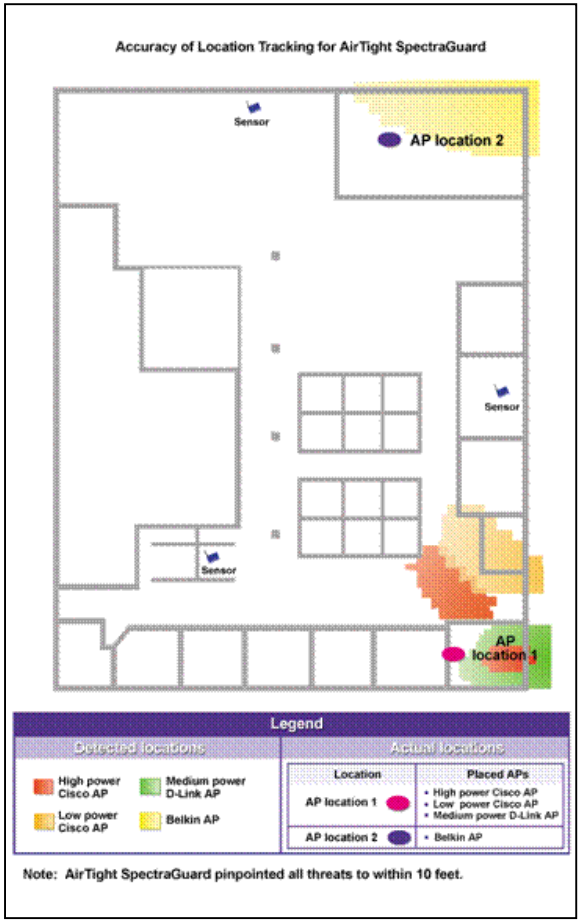
Sensitive to signal variations resulting in inaccurate location tracking

Requires site survey for calibration

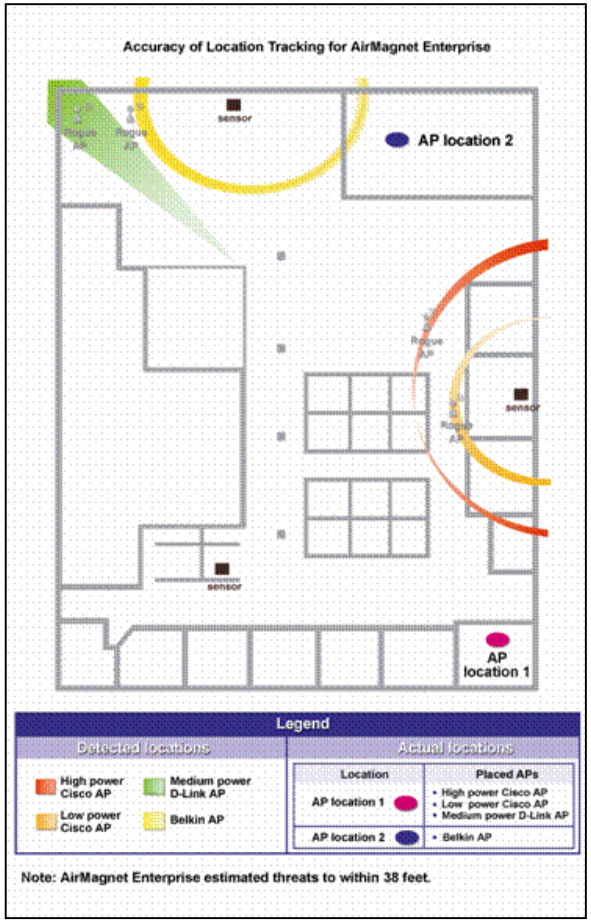
Best Threat Detection and Prevention



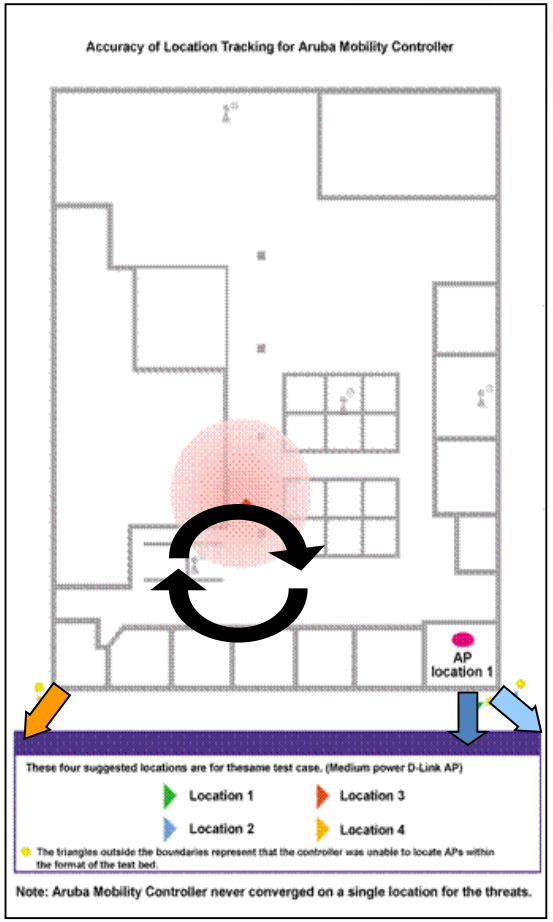
Most Accurate Location Tracking



AirTight



AirMagnet



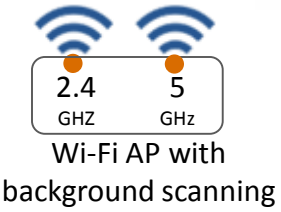
Aruba

* Aruba repeatedly rotated through 4 locations for a single threat

AirTight WIPS Flavors

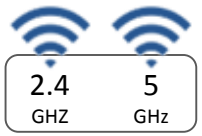
WIPS Architectures

- **Integrated**
  - APs repurposed as sensors for background scanning
  - Full threat detection and wire-side Rogue AP prevention
  - Not recommended with time-sensitive apps, e.g., VoIP

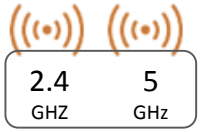


Wi-Fi AP with
background scanning

- **Overlay**
  - Dedicated sensors on top of existing WLAN
  - 24/7 monitoring and protection

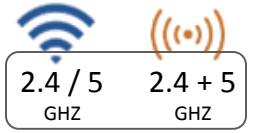


Wi-Fi AP



WIPS Sensor

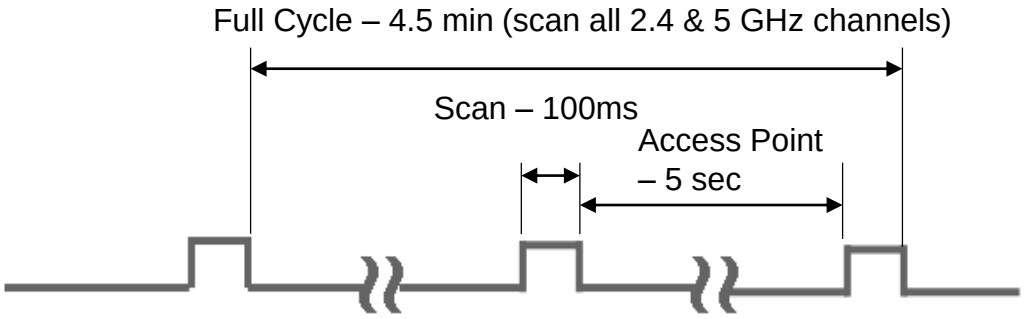
- **Combo**
  - APs repurposed as sensors
  - 24/7 monitoring and protection
  - Able to support all types of apps, including VoIP



Wi-Fi AP with
Concurrent WIPS sensor

Integrated / Background WIPS

- Scans all 2.4 and 5 GHz band channels
- Monitors 8 VLANs for rogue APs using Marker Packet™
  - Patented packet injection time-synchronized with off-channel visits for reliable detection of Rogue APs
- Automated wire-side prevention of unlimited number of Rogue APs
- Works even with unmanaged switched
- Detects over-the-air policy violations, e.g., client mis-associations, ad-hoc connections



AT-C60: Industry's Most Flexible Wi-Fi Platform

- Software-defined, band-unlocked radios – an industry first
- Concurrent Wi-Fi access and 24/7 WIPS – an industry first

AirTight WIPS Platforms

AirTight Deployment Choices

Platforms


AT-C10


AT-C50


AT-C60


AT-C55

Deployment


Public Cloud


VMware


Private Cloud


Appliance

Pricing

- ✓ Zero Capex
- ✓ Bundled
- ✓ Capex

No feature based licensing!
No user based licensing!

AirTight Server Appliances

SA-250
Standard Appliance

SA-360
Premium Appliance

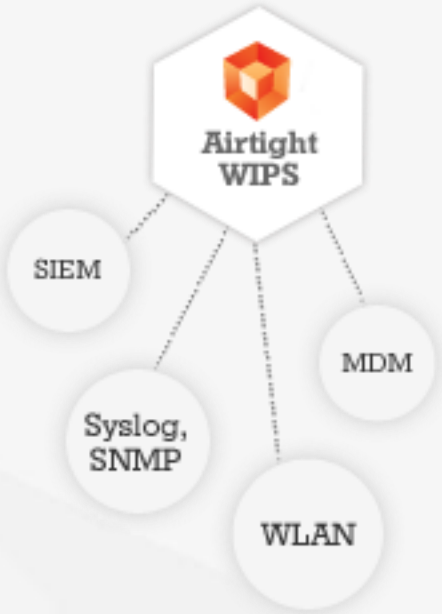
AirTight Access Points





C-50	C-55 and C55-E	C-60	0-70 (outdoor)	C-75 and C-75-E
Single “n” radio	Dual “n” radio	Dual “n” radio	Dual “n” radio	Dual “ac/n” radio
2x3:3	2x2:2 2x2:2	3x3:3 2x2:2	3x3:3 3x3:3	3x3:3 3x3:3
300 Mbps	300 Mbps 300 Mbps	450 Mbps 300 Mbps	450 Mbps 450 Mbps	1.3 Gbps “ac” 450 Mbps “n”
• Single AP • Single WIPS	• Dual AP • Dual WIPS	• Dual AP • Dual WIPS • 1 AP, 1 WIPS	• Dual AP • Dual WIPS	• Dual AP* • Dual WIPS (Phase 2)
PoE	PoE	PoE	PoE+	PoE

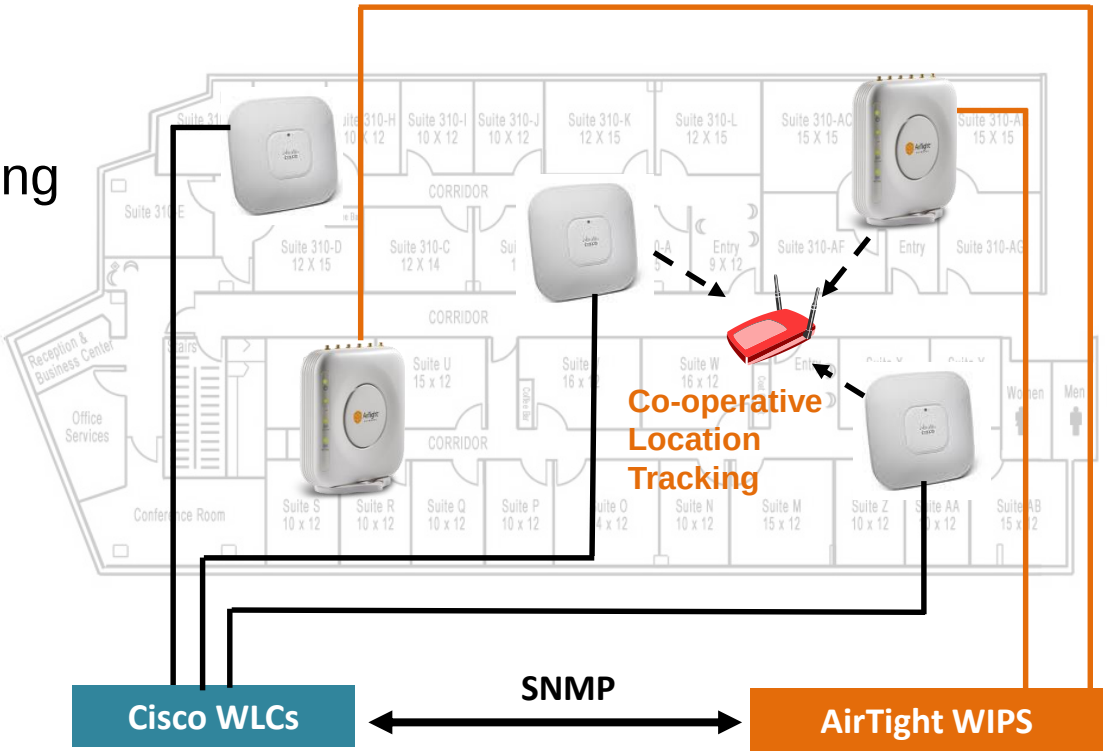
Integration with 3rd Party Systems



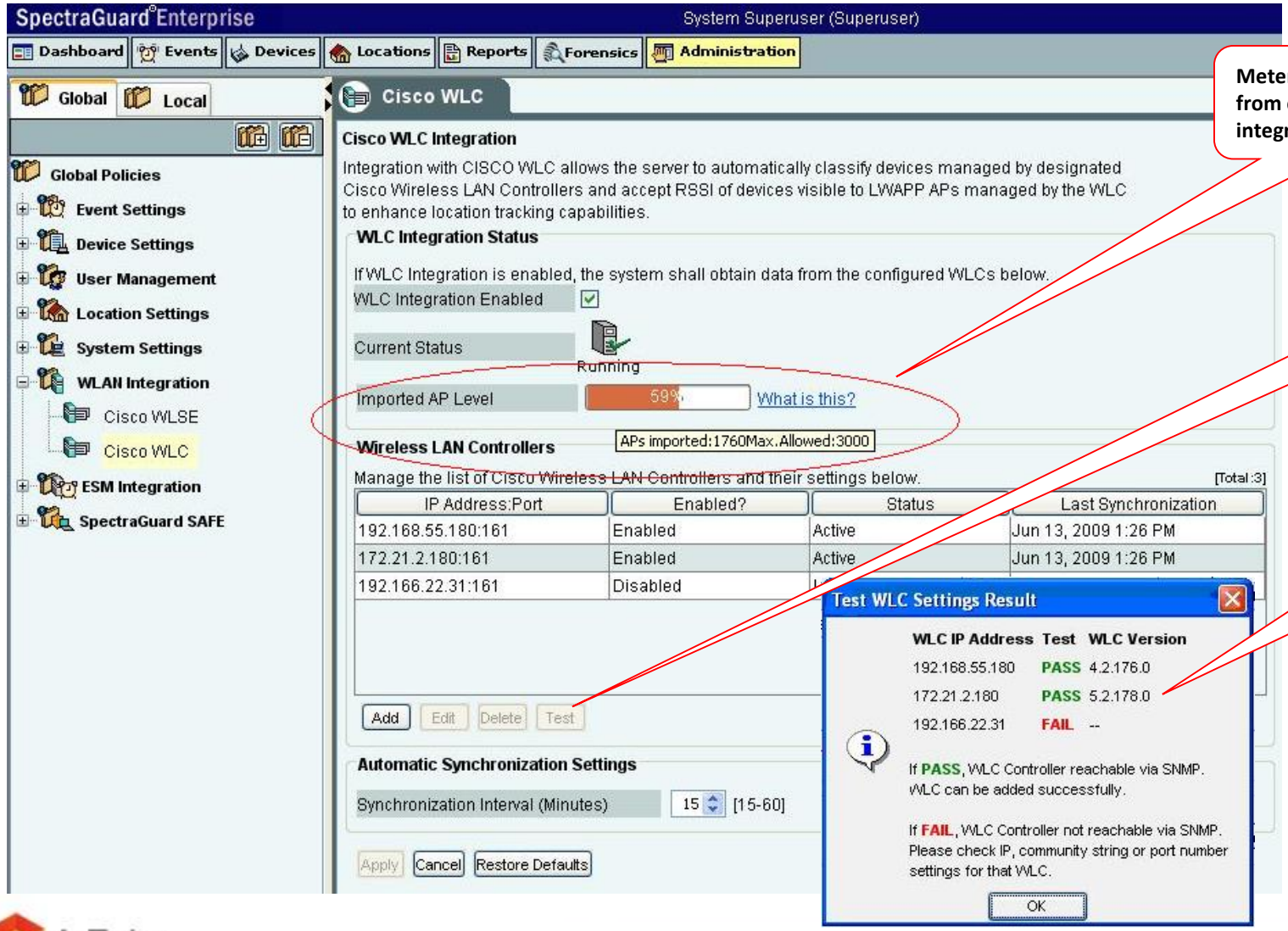
Comprehensive Enterprise Integration

Cisco WLC Integration

- Synchronize devices between Cisco WLCs and AirTight WIPS
  - Automatically identify and populate managed AP information in WIPS
- Use AirTight auto-classification, prevention, location tracking
- Reduces WIPS sensor density for location tracking
  - Use RSSI information from APs along with WIPS sensors



Cisco WLC Integration

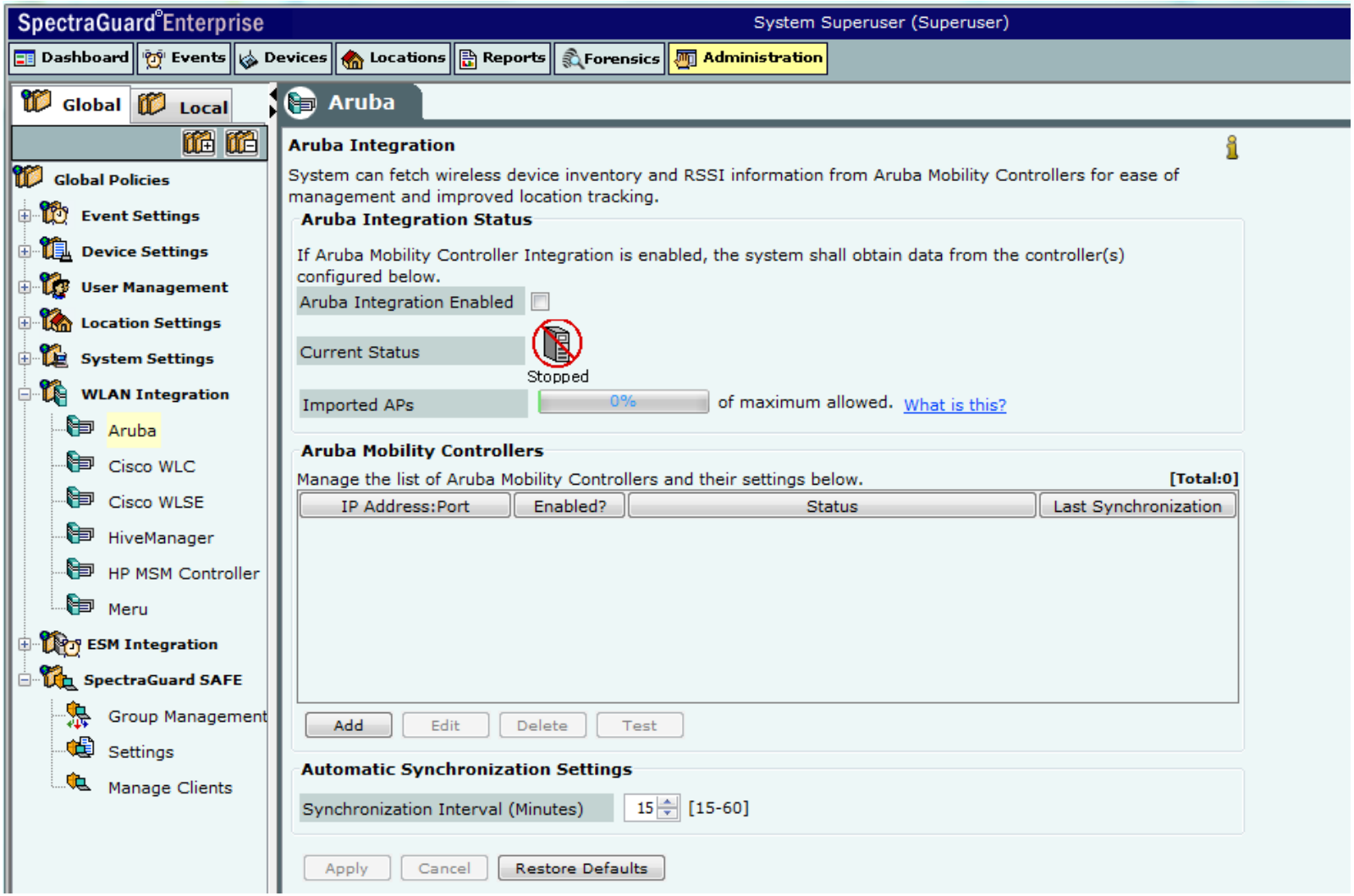


Meter to show the load from existing WLC integrations

Test function shows status of the configuration of each WLC controller

Added Support for WLC v5.2 and v6.0

Aruba Mobility Controller Integration



Secure BYOD Onboarding via MDM Integration

AirTight WIPS

MDM Server

1 Import list of approved smart devices

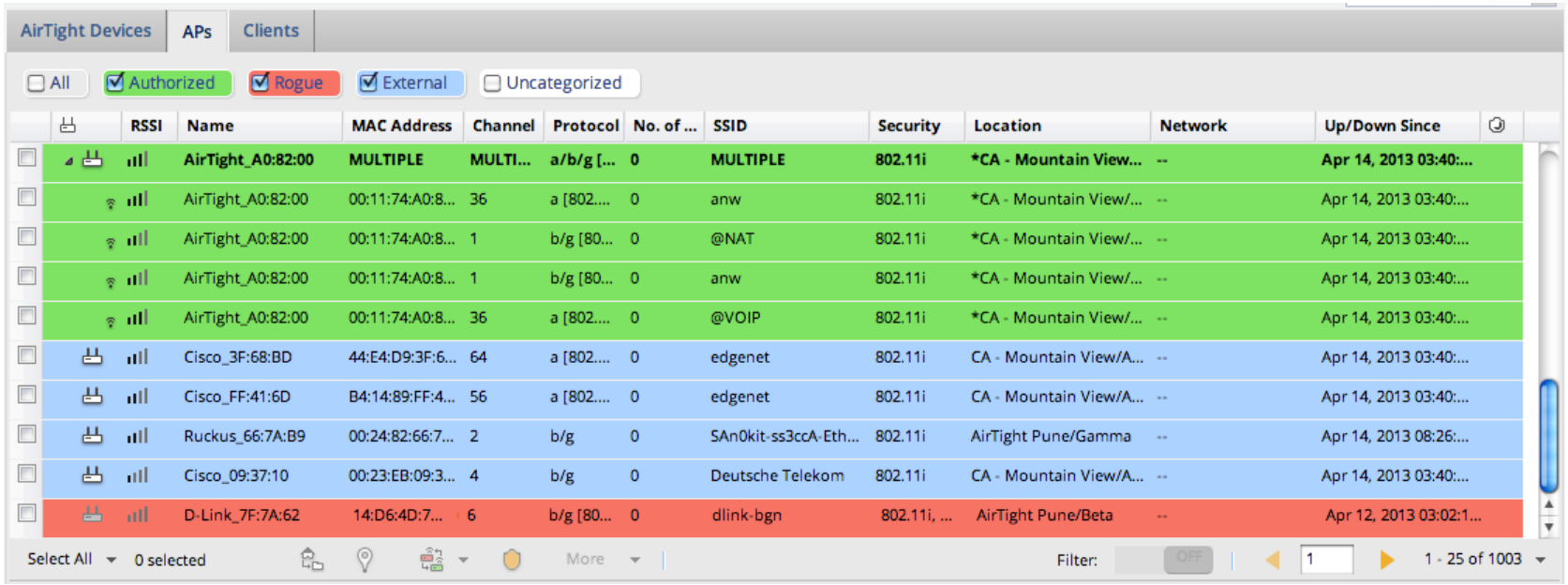
2 Automatically quarantine unapproved smart devices from connecting to enterprise Wi-Fi

3 Users must get MDM agent installed on personal devices for approved usage

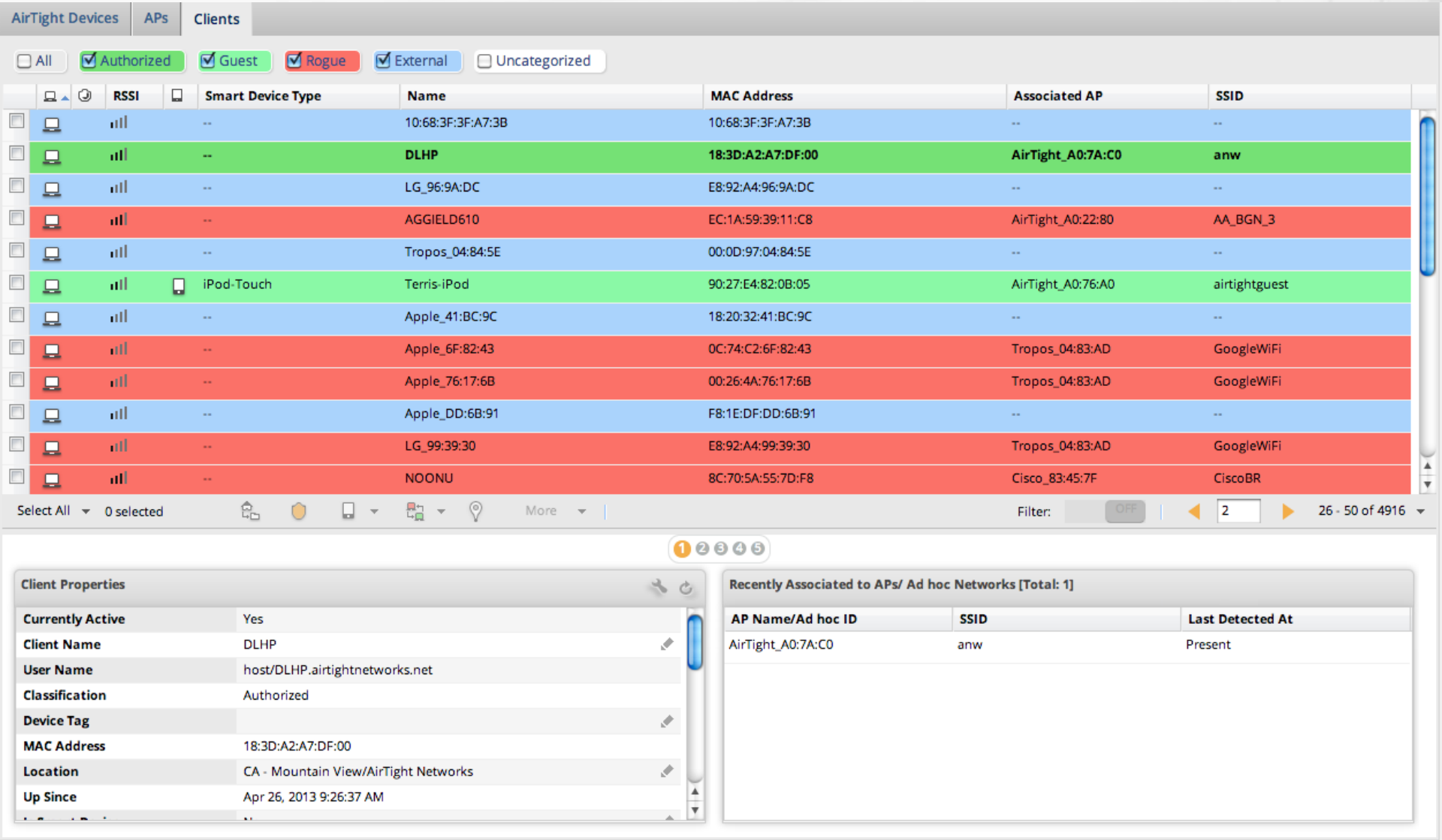
Employee-owned smartphones and tablets

AirTight WIPS Screenshots

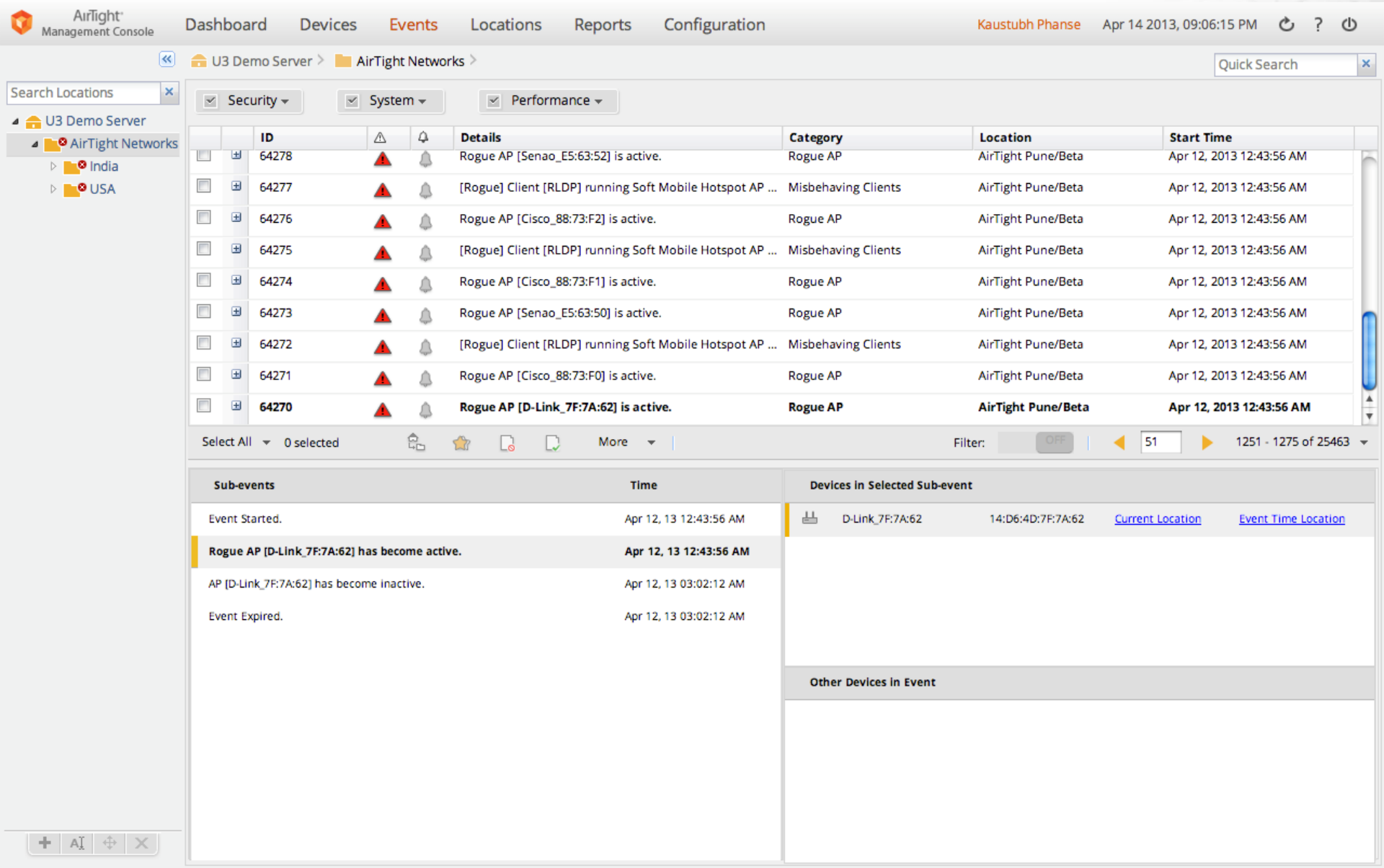
Automatic AP Classification



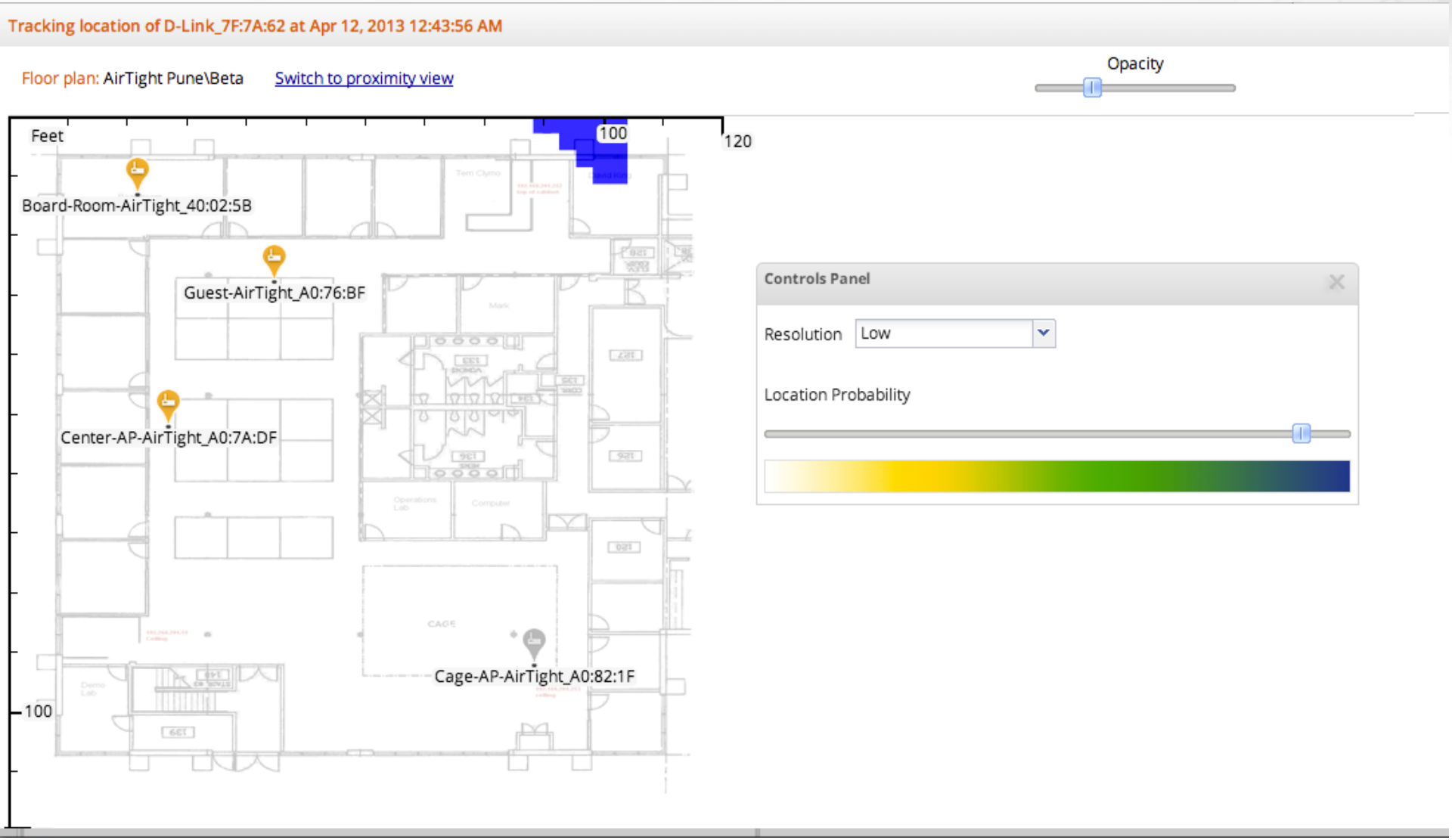
Automatic Client Classification



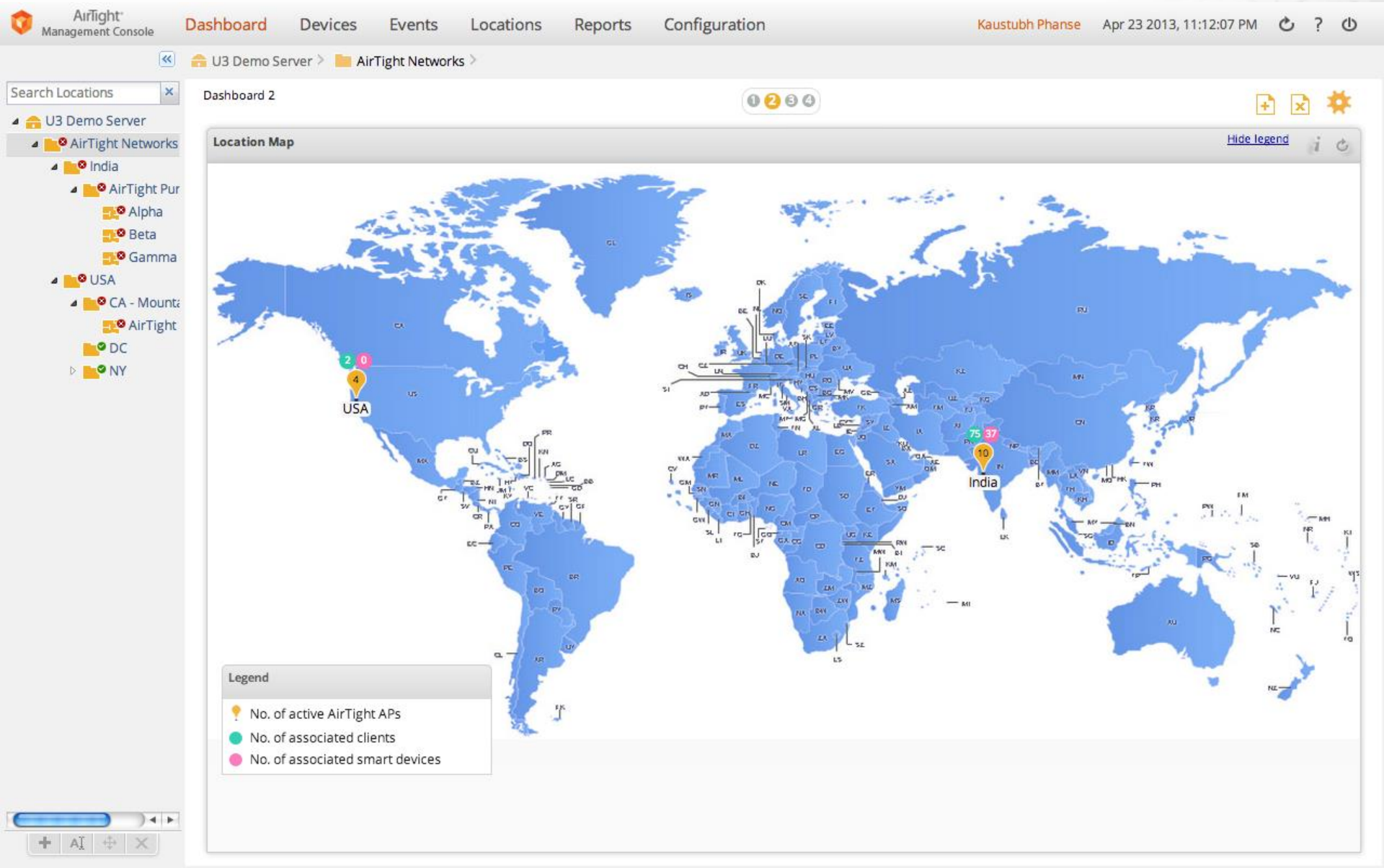
Wireless Security Alerts



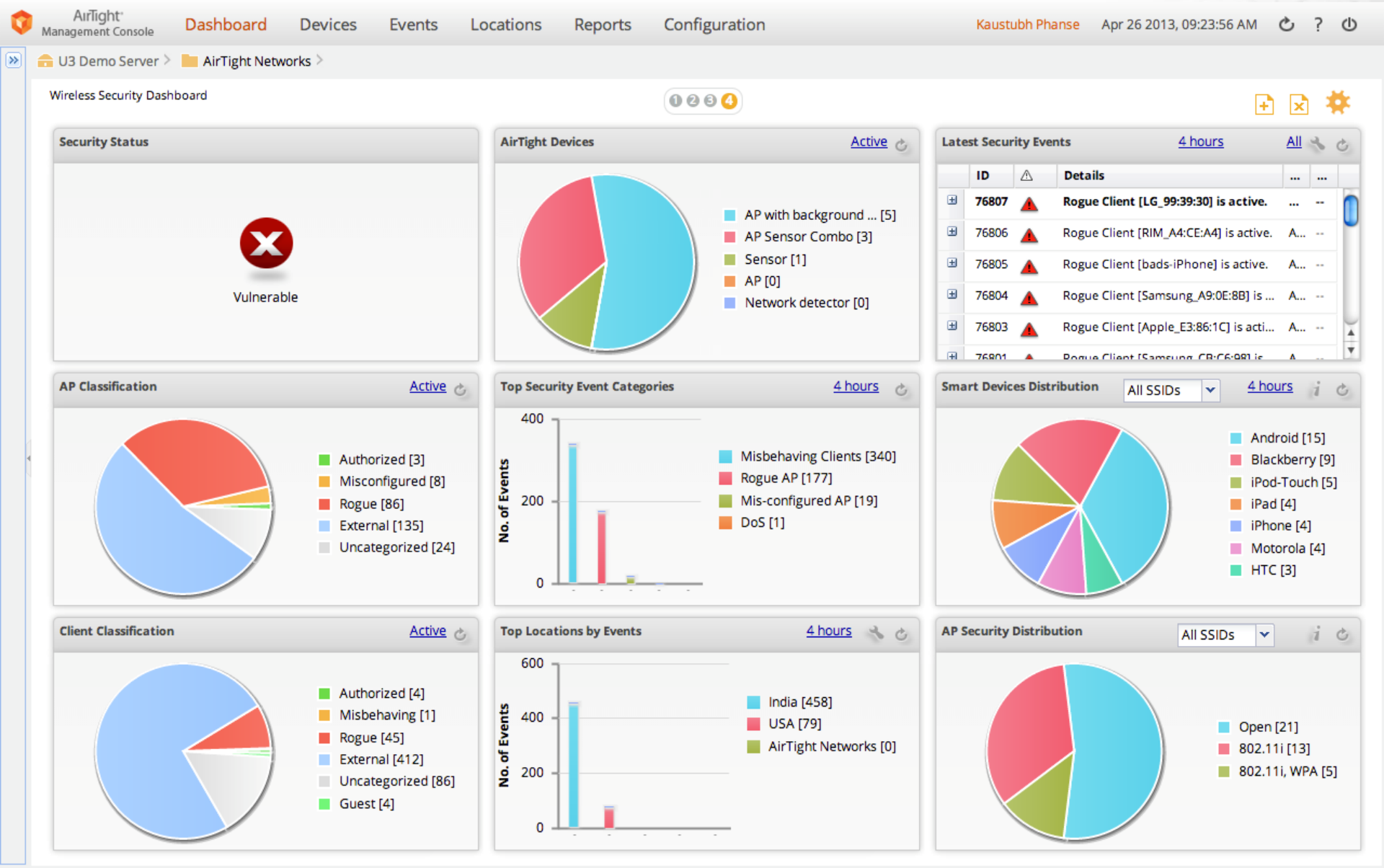
Rogue AP Location Tracking



Dashboard


AirTight Management Console
Dashboard
Devices
Events
Locations
Reports
Configuration
Kaustubh Phanse
Apr 23 2013, 11:12:07 PM
U3 Demo Server
AirTight Networks
Search Locations
U3 Demo Server
AirTight Networks
India
AirTight Pur
Alpha
Beta
Gamma
USA
CA - Mountz
AirTight
DC
NY
Dashboard 2
Location Map
Hide legend
2
0
4
USA
75
37
10
India
Legend
No. of active AirTight APs
No. of associated clients
No. of associated smart devices

WIPS Dashboard



Secure Enterprise WLAN Checklist

Can your enterprise WLAN solution:

- ✓ Accurately detect all types of Rogue APs without you having to define any signatures?
- ✓ Not flood you with false alerts?
- ✓ Let you reliably turn on the P in WIPS?
- ✓ Automate BYOD policy enforcement and onboarding?
- ✓ Accurately track physical location of detected Wi-Fi devices?
- ✓ Do all of the above without compromising on Wi-Fi access features and ripping off your IT budget?

Thank You!

Cloud Managed Secure Wi-Fi Solutions

Tom Haak
Director Sales

Konrad-Zuse-Platz 8
81829 Munich
Germany

P. +49 89 207042400
M. +49 179 2414200
E. tom.haak@airtightnetworks.com

Leo Sterr
Senior Sales Engineer

Konrad-Zuse-Platz 8
81829 Munich
Germany

P. +49 89 207042401
M. +49 151 12197767
E. leo.sterr@airtightnetworks.com